S-246867

No.

Vancouver Registry

IN THE SUPREME COURT OF BRITISH COLUMBIA

Between

[redacted] PATTERSON

PLAINTIFF

and

SNOWFLAKE INC.,
LIVE NATION ENTERTAINMENT, INC.,
LIVE NATION CANADA, INC.,
TICKETMASTER LLC,
TICKETMASTER CANADA LP,
TICKETMASTER CANADA HOLDINGS ULC
-and- TICKETMASTER CANADA ULC

DEFENDANTS

Brought under the *Class Proceedings Act*, R.S.B.C. 1996, c. 50

NOTICE OF CIVIL CLAIM

(SNOWFLAKE, LIVENATION AND TICKETMASTER – Data Security Breach)

This action has been started by the plaintiff for the relief set out in Part 2 below.

If you intend to respond to this action, you or your lawyer must

(a) file a response to civil claim in Form 2 in the above-named registry of this court within the time for response to civil claim described below, and

(b) serve a copy of the filed response to civil claim on the plaintiff.

If you intend to make a counterclaim, you or your lawyer must

(a) file a response to civil claim in Form 2 and a counterclaim in Form 3 in the above-named registry of this court within the time for response to civil claim described below, and

(b) serve a copy of the filed response to civil claim and counterclaim on the plaintiff and on any new parties named in the counterclaim.

JUDGMENT MAY BE PRONOUNCED AGAINST YOU IF YOU FAIL to file the response to civil claim within the time for response to civil claim described below.

Time for response to civil claim

A response to civil claim must be filed and served on the plaintiff,

(a) if you reside anywhere in Canada, within 21 days after the date on which a copy of the filed notice of civil claim was served on you,
(b) if you reside in the United States of America, within 35 days after the date on which a copy of the filed notice of civil claim was served on you,
(c) if you reside elsewhere, within 49 days after the date on which a copy of the filed notice of civil claim was served on you, or
(d) if the time for response to civil claim has been set by order of the court, within that time.

THE PLAINTIFF'S CLAIM

PART 1: STATEMENT OF FACTS

Overview

1. The Applicant wishes to institute a class action on behalf of the following class, of which he is a member, namely:

> All persons resident in Canada, excluding Quebec, whose personal information was subject to unauthorized access in the cyber incident disclosed in Defendant Live Nation Entertainment's filing with the U.S. Securities and Exchange Commission dated May 31, 2024.

2. This case concerns the Defendants' negligence in failing to adequately protect and safeguard Class Members' private personal and personal information by allowing or otherwise failing to prevent its theft as part of massive cyber incident and data breach.

3. As revealed in the Defendant Live Nation Entertainment's filing for the U.S. Securities and Exchange Commission dated May 31, 2024, said Defendant "identified unauthorized activity" within Snowflake's "third-party cloud database environment containing

Company data (primarily from its Ticketmaster LLC subsidiary)" on May 20 and May 27, 2024.[1] Said database is owned and operated by Defendant Snowflake, Inc.

4. The Defendant's SEC filing also revealed that "[on] May 27, 2024, a criminal threat actor offered what it alleged to be Company user data for sale via the dark web." The "Company user data" refers to the private and personal information compromised in the cyber incident.

5. The private and personal information compromised in the data breach extends to names, addresses, phone numbers, credit card and debit card information of Ticketmaster users and customers around the world – including users resident in British Columbia. Approximately 560 million Ticketmaster account holders and users were impacted by the data theft incident. A total of 1.3 terabyte of personal and private information was stolen.

6. These numbers make the data breach the most significant data breach in history in terms of individuals affected and extent of data stolen.

7. While the vast majority of the data breached was from customers and users located in the United States, Canadians were the second-largest demographic group.

8. The Live Nation-Ticketmaster Defendants' negligence is compounded by their failure to provide timely notice of the data-compromising cyber-incident to Class Members, its occurrence, nature, or extent.

9. In fact, the Live Nation-Ticketmaster Defendants only notified Canadian users and consumers in an email dated July 9, 2024, over one month after the cyber incident was first publicly revealed in Live Nation's SEC filing dated May 31, 2024. In this letter,

1 Public clouds are computing resources and data storage and protection services maintained by a third party – such as Snowflake – rather than by the company owning the data. Public cloud are not dedicated to any particular customer; instead, customers such as Live Nation essentially "lease" space from the public cloud service provider.

the Defendants also revealed that the data breach occurred between April 2 and May 18, 2024.

10. Class Members entrusted their most sensitive data – data that could be used by cyber and/or real-world criminals to steal their identities – to Live Nation/Ticketmaster and the cloud computing company they contracted based on their reasonable belief that it would be safe and secure.

11. This case is about Live Nation, Ticketmaster, and Snowflake's conduct – not the data theft that revealed it. To obtain customer data and the lucrative interest and fees those customers generated, said Live Nation-Ticketmaster promised customers that their data would be safe and protected in Snowflake's public cloud data storage environment. These assurances have now been shown to be indisputably false and/or misleading – and they continue to be so.

12. As a result of the Defendants' false and/or misleading representations regarding the safety of the data under their control and/or in their possession, Class Members have paid millions of dollars in fees to Live Nation and Ticketmaster that they never would have paid had they known the truth: that their sensitive personal and private data was being pooled in a giant "data lake" on Snowflake's public cloud.

13. The Live Nation-Ticketmaster Defendants have purchased a 12-month identity monitoring subscription for affected users and customers from TransUnion. This is, however, insufficient because several banking and financial institutions do not report to TransUnion, including TD Bank, CIBC, Desjardins and HSBC. As well, the 12-month period is too short and shorter than the 2-year coverage purchased for individuals affected by previous large-scale data security incidents involving the theft and compromise of sensitive financial and personal data.

14. The Applicant and Class Members suffered and will foreseeably continue to incur significant tangible compensable injuries directly and immediately caused by the

Defendants' negligent violations of their privacy rights, and are entitled to claim damages for, *inter alia*:

(a) Additional credit monitoring services/identity theft protection services not covered by the Defendants;

(b) Trouble and inconvenience by having to carefully review their transactions and credit card accounts and be on the lookout for fraud,

(c) The lost inherent value of their personal and private information, which they had been unaware was subject to unlawful access and use,

(d) The trouble and inconvenience of having had private and personal information compromised,

(e) Identity theft and future fraud resulting from the theft of their personal and private information,

(f) Possible future fraud and identity theft by third parties and injury flowing from therefrom,

(g) Costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts,

(h) Lower credit scores resulting from credit inquiries following fraudulent activities,

(i) Costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to mitigate and address the actual and future consequences of the data theft, including discovering fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft

protection services, and the stress, nuisance, anxiety and annoyance of dealing with the repercussions of the data theft,

(j) Pain, suffering, stress, and anxiety, and

(k) Punitive damages.

The Parties

15. Defendant Snowflake Inc. is a corporation legally constituted under the laws of Delaware and headquartered in Bozeman, MT. Snowflake Inc. is a cloud computing-based data cloud company that other companies contract with for, *inter alia*, data storage and protection services.

16. Defendant Live Nation Entertainment Inc. ("Live Nation") is a corporation duly constituted under the laws of Delaware and headquartered in Beverly Hills, CA. Live Nation Entertainment Inc. was founded in 2010 following the merger of Live Nation, Inc. and Ticketmaster Entertainment LLC. Live Nation trades publicly on the New York Stock Exchange (NYSE: LYV).

17. Defendant Live Nation Canada, Inc. is a corporation duly constituted under the laws of Ontario and headquartered in Toronto, ON. Live Nation Canada, Inc. is a wholly owned subsidiary of Live Nation. On January 1, 2024, Live Nation Canada, Inc. absorbed Live Nation Touring (Canada), Inc.

18. Defendant Ticketmaster LLC is a limited liability company duly constituted under the laws of Virginia and headquartered in Beverly Hills, CA. Ticketmaster Entertainment LLC is a wholly owned subsidiary of Live Nation. Ticketmaster Entertainment, LLC is a ticket sales and distribution company.

19. Defendants Ticketmaster Canada Holdings ULC, Ticketmaster Canada LP, and Ticketmaster Canada ULC (referred to herein as "Ticketmaster Canada") are all legal persons constituted under the laws of Canada.

20. Ticketmaster Canada Holdings ULC is a corporation constituted under the *Canada Business Corporations Act* and is owned by Live Nation Luxembourg Holdco 2 S.A.R.L., a corporation based in the Grand Duchy of Luxembourg.

21. Ticketmaster Canada LP is a limited partnership constituted under the laws of Ontario, and its parent company is Ticketmaster Canada Holdings ULC.

22. Ticketmaster Canada ULC is a corporation constituted under the laws of Nova Scotia, and its parent company is Ticketmaster Canada LP.

23. The Plaintiff brings this claim on their own behalf and on behalf of all persons resident in Canada, excluding Quebec, whose personal information was subject to unauthorized access in the cyber incident disclosed in Defendant Live Nation Entertainment's filing with the U.S. Securities and Exchange Commission dated May 31, 2024 (the "**Class**", "**Class Members**" and "**Class Period**").

24. In light of the foregoing, all Defendants are solidarily liable for the acts and omissions of the other.

25. Excluded Persons means: (1) Directors and officers of the Defendants and their immediate families; and (2) Counsel for the parties, and the case management judge and trial judge in this proceeding, and their immediate families.

26. The Plaintiff is a resident the City of Burnaby, British Columbia. He has been a Ticketmaster account holder for at least fifteen years and has paid for tickets to attend several Ticketmaster / Live Nation events. As part of account creation and in using his

account over the years, the Plaintiff provided personal, financial, and other information to Ticket Master / Live Nation including his name, address, email, and credit card numbers.

27. On July 9, 2024, the Plaintiff received an email from Ticketmaster / Live Nation informing him of a cyber incident involving a data breach leading to the compromise of his personal information, including financial information registered to his account.

28. The email informed him that Ticketmaster / Live Nation would be paying for a one-year subscription for credit monitoring services purchased on his behalf from TransUnion.

29. The process required for the Plaintiff to activate access to the subscription for him to visit the link provided in the Ticketmaster / Live Nation website and to enter his email address, after which he would receive an activation code to be entered on the TransUnion website. At the time of filing the present Notice of Civil Claim, on October 7, 2024, the Plaintiff is still waiting for the email containing said activation code and received further notification that he would not be receiving the activation code for another "few weeks."

30. The Plaintiff is aware that the credit monitoring services paid for on his behalf is for a duration shorter than the industry standard of two years that is usually purchased by entities on behalf of individuals affected by a data breach. The Plaintiff is also aware that the credit monitoring provided by TransUnion is inadequate, ineffective, insufficient, and deficient for this reason and because several major banking and other financial institutions do not report to TransUnion including TD, CIBC, and HSBC.

31. As a result, on October 4, 2024, the Plaintiff purchased an additional credit monitoring subscription service from Equifax Canada for a period of two years, namely, Equifax Complete Premier. The subscription paid for by the Plaintiff is $26.20 per month.

The Situation

32. This class action concerns a cyber incident leading to the compromise of the personal and private information of an estimated 560 million account holders and other users of Ticketmaster's website, application, and in-person points-of-sale that the Defendants Live Nation and Ticketmaster organized to have stored on Defendant Snowflake Inc.'s third-party cloud-based data storage and protection services.

33. As highlighted in a Press Release from the US Department of Justice issued May 23, 2024, Live Nation describes itself as the "largest live entertainment company in the world," the "largest producer of live music concerts in the world," and "the world's leading live entertainment ticketing sales and marketing company".

34. As also highlighted in the US DOJ's Press Release, Live Nation owns or controls more than 265 concert and event venues in North America, including more than 60 of the top 100 amphitheaters in the United States. Live Nation generates $22 billion globally in annual revenue from business segments: concerts (e.g. promotions, venue management, and music festival production), ticketing (e.g. Ticketmaster business), and sponsorship and advertising.

35. Ticketmaster sells concert tickets to interested parties when tickets are first made available for purchase and operates resale platforms on which purchasers can resell tickets at a later time.

36. As also highlighted in the DOJ Press Release, "Ticketmaster is by far the largest concert ticketing company in the United States, multiple times the size of its closest competitor".

37. Live Nation's website also boasts as follows:

> Ticketmaster is the global leader in ticket management for largescale sports and entertainment, specializing in sales, marketing and distribution. As the largest marketplace in the world, Ticketmaster is also the number one event search platform trusted by billions of live event fans.

38. Ticketmaster is the largest and often the exclusive primary seller of tickets for events in Canada and British Columbia.

39. The Privacy Policy featured on the Ticketmaster.ca website to be used by actual and prospective users situated in Canada and British Columbia provides as follows:

> **WHO WE SHARE YOUR DATA WITH & WHY**
>
> **Third parties who perform services on our behalf.**
>
> Our third-party service providers, some of which may be located outside of your jurisdiction. These include:
>
> Cloud hosting providers, who provide the IT infrastructure on which our global products and systems are built;
>
> [...]
>
> Information security providers, who help us keep our platforms safe and secure [...] (emphasis added)

40. The Defendant Snowflake Inc. is one of Live Nation-Ticketmaster's third-party service providers, providing public cloud services for the storage and protection of customer and user data collected and generated by Live Nation-Ticketmaster in the sale, purchase and transfer of tickets, and transferred to Snowflake.

41. The data transfer policy that appears on the Ticketmaster.ca website used by Class Members and other Canadians confirms that the personal and private information of Ticketmaster customers and users located in British Columbia and the rest of Canada is transferred to third-party service providers around the world, including the United States. This necessarily includes transfers of personal and private customer information for third-party cloud storage services provided Snowflake Inc:

> **Data Transfers**
>
> As part of a global group of companies headquartered in the United States, we may need to transfer your information outside of your country of residency. This occurs where:
>
> [...]

> We use global service providers, such as the ones noted above.
>
> When transferring information, there are strict rules in place to ensure your data is still protected to the highest standard. Where we do this, we will ensure that appropriate safeguards are put in place. Where your information is transferred outside of your local market, we use contractual measures and internal mechanisms requiring the recipient to comply with the privacy standards of the exporter, we will use one of the mechanisms listed below [listing Contractual Clauses, Binding Corporate Rules and Binding Corporate Processor Rules].

42. As seen above, Live Nation-Ticketmaster also represents to its customers that transfers of personal and private customer information are subject to "strict rules in place to ensure [the] data is still protected to the highest standard" and that "appropriate safeguards are put in place."

43. The lack of safety and security in LiveNation-Ticketmaster's practices of personal and private information retention, transfer and storage, and that of Snowflake Inc. as Live Nation-Ticketmaster's provider cloud-based storage services is at the heart of the present proposed class action.

44. Live Nation's filing for the US Securities and Exchange Commission dated May 31, 2024 "identified unauthorized activity" within Snowflake's "third-party cloud database environment containing Company data (primarily from its Ticketmaster LLC subsidiary)" on May 20, 2024.

45. Live Nation's SEC filing also revealed that "[on] May 27, 2024, a criminal threat actor offered what it alleged to be Company user data for sale via the dark web." The "Company user data" refers to the private personal and payment information compromised in the cyber incident.

46. Live Nation's SEC filing did not identify Snowflake as the provider of the "third party cloud database environment". However, a Ticketmaster spokesperson confirmed on May 31, 2024, that its stolen database was hosted by Snowflake, as appears in an article published by Tech Crunch on that date.

47. Further, Snowflake's Chief Information Security Officer, Brad Jones, acknowledged the cybersecurity incident in a blog post on Snowflake's website published on May 31, 2024. The blog post also refers to its "ongoing investigation involving a targeted threat campaign against some Snowflake customer accounts".

48. On May 27, 2024, a newly registered account on the cybercrime forum Exploit posted an advertisement offering for sale 1.3 terabytes of personal and private information of over 560 million Ticketmaster users and customers in exchange for $500,000 USD ($680,000 CDN). These numbers make the May 2024 data breach the most significant data breach in history in terms of individuals affected and extent of data stolen.

49. As highlighted in a WIRED article, a hacking group self-identifying as responsible for the data breach, ShinyHunters, posted an identical advertisement on its own website, Breach Forums, on May 28, 2024.

50. The Live Nation-Ticketmaster Defendants only notified Canadian users and consumers in an email dated July 9, 2024, over one month after the cyber incident was first publicly revealed in Live Nation's SEC filing dated May 31, 2024. In this email, the Defendants also revealed that the data breach occurred between April 2 and May 18, 2024.

51. Importantly, the Defendants' email does not provide any explanation for the delay between discovering the cyber incident, and the day on which Plaintiff and Class Members were actually notified. The email does, however, specify that "this notice has not been delayed due to law enforcement investigation." (emphasis added).

52. The personal and private information compromised in the data breach extends to names, addresses, email addresses, phone numbers, and credit card and/or debit card information of Ticketmaster users around the world – including users resident in British Columbia.

53. Ticketmaster's personal information retention policy for Canada provides that Ticketmaster retains customers personal and private information for an indefinite period

as long as an account remains active, and for at least seven years following an account becoming inactive, unless the customer deletes their account at an earlier time.

54. Ticketmaster's personal information retention policy is contained in its Privacy Policy. Relevant parts are as follows:

> How long do we retain your personal information?
>
> **Your Ticketmaster Account.** Your account is your digital identity on Ticketmaster; it is how we ensure your ticket purchases are secure and connected to an individual. It is also the primary basis for determining how long we keep your information.
>
> Whenever you purchase a ticket, log into your account, or interact with us, we log this activity. So long as your account remains active we will continue to retain the information we have processed about you. For example we will:
>
> - Retain your purchases or favorites so we can recommend relevant events;
> - Keep your tickets assigned to you, so we continue to deliver events to true fans; and
> - Keep your account validated and secure.
>
> Your information will be deleted if you either (1) request deletion of your account, in which case your account and associated information will be deleted within a maximum of 90 days depending on the timeframes required by your local laws; or (2) your account has 7 years' of inactivity.
>
> Aside from this account-based rule, the retention of your information is also determined on the following bases:
>
> **To provide you with the services you have requested.** For example, when you purchase tickets or services from us, we cannot delete your account while you have an upcoming event, as you would not be able to attend the event you have purchased.
>
> **When a law requires us to retain your information.** For example, we retain certain purchase information for accounting and tax purposes even after you have deleted your account.
>
> **When we have processed certain data with your consent.** For example, if you have provided us with details of your accessible

needs, if you withdraw your consent to this processing, we would delete that information.

Safety & Security. We also maintain limited information in separate databases to keep our platforms safe and secure, such as to detect and prevent fraud, to power cyber security protections and to enforce our terms and any attempt to circumvent them.

55. As also stated in the Privacy Policy accessible on the Ticketmaster.ca website used by Class Members and other Canadian residents, Ticketmaster Canada is responsible for processing data from Canadian customers and users of Ticketmaster's mobile application and website. However, the information collected by Ticketmaster.ca is further processed by other entities constituting the "Ticketmaster family of companies, including in the United States":

> **Ticketmaster entities per country**
> The data controller that processes your data depends on which market you have an account or subscription with. The Ticketmaster family of companies also provides support services on behalf of one another and therefore acts as processors on behalf of the data controller to whom you have provided your data.

56. The personal and private information of Class Members collected by Ticketmaster Canada and compromised in the breach of Snowflake's cloudbased environment was therefore either directly transferred to Snowflake by Ticketmaster Canada, or by one of the other companies constituting the Ticketmaster family of companies.

57. Live Nation-Ticketmaster negligently assessed the safety and security of its third-party cloud-based data storage and protection service provider, the Defendant Snowflake.

58. Live Nation-Ticketmaster negligently or fraudulently misrepresented the safety and security of its third-party cloud-based data storage and protection service providers, including the Defendant Snowflake. Live Nation-Ticketmaster thereby violated the requirement in consumer protection legislation that the services provided conform to the statements or advertisements regarding them made by the merchant and the warranties it made of Ticketmaster being a "safe and secure platform" for purchasing tickets.

59. Ticketmaster expressly represented and continues to represent that Ticketmaster is a "safe and secure platform" for the purchase of tickets. The May 2024 cyber incident shows this not to be true. This conduct further violates the prohibition of false or misleading representations in consumer protection legislation.

60. In addition, Live Nation-Ticketmaster negligently selected Snowflake as its vendor and provider of third-party public cloud data storage services despite Snowflake not requiring multi-factor authentication for accessing customer credentials and accounts or data stored on the cloud, or taking additional measures to protect credentials, accounts and/or data subject to single-factor authentication.

61. Live Nation-Ticketmaster was also negligent in failing to require and ensure that all accounts and credentials for accessing its account and data stored on Snowflake's cloud environment were protected by multi-factor authentication. As Snowflake itself highlighted in its press release, the data breach "appears to be a targeted campaign directed at users with single-factor authentication".

62. Snowflake was negligent in failing to design a cloud-based data storage environment that did not expose the personal and private information of their clients' customers and users to cyber attacks resulting in data theft.

63. As Snowflake's Chief Information Security Officer stated in his blog post, if a "threat actor obtains customer credentials, they may be able to access the account." However, Snowflake failed to adopt or failed to adopt effective policies and measures to prevent information-stealing malware from obtaining their customers' credentials and/or preventing the unlawful accessing of personal and private information of their customers' own customers and users stored on Snowflake's cloud-based data storage environment.

64. For example, Snowflake did not require its customers to set up multi-factor authentication for accessing their accounts and data stored in the cloud. Snowflake did not require that the entering of valid account credentials trigger a further requirement to authenticate the

lawful and authorized access by entering a code received on the cellular phone associated with the account.

65. As noted, the blog post from Snowflake's Chief Information Security Officer produced highlighted that the data breach incident "appears to be a targeted campaign directed at users with single-factor authentication" and recommended that "organizations immediately… Enforce Multi-Factor Authentication on all accounts".

66. Snowflake failed to exercise the necessary prudence and diligence despite being aware of the risks that single-factor authentication posed a risk for the safety and security of customer credentials, accounts and data stored on third-party public cloud environments. In a Knowledge Base Article published on its website on June 2, 2024, Snowflake acknowledged that the data breach "is the result of ongoing industry-wide, identity-based attacks with the intent to obtain customer data".

67. Snowflake was furthermore negligent in failing to notice and address the vulnerabilities and risks associated to customer accounts and data not subject to multi-factor authentication or to take effective steps to address them.

68. As acknowledged by Snowflake's Chief Information Security Officer in his blog post, Snowflake first became aware of the suspicious activity on May 23 but later discovered that the information-stealing, credential compromising, and data theft activities had been happening since mid-April. Cyber criminals were therefore able to access and steal data stored on Snowflake's cloud by numerous customers without any hindrance or detection for over 1 month.

69. Snowflake's customers were not notified and were therefore prevented from taking measures to protect their customers' data stored on Snowflake's cloud environment, including selecting a more secure provider of cloud storage services.

70. Snowflake was also negligent in failing to inquire into whether customer credentials and accounts were protected by multi-factor authentication and other methods of protection, or otherwise took steps to prevent the vulnerabilities exploited in the data breach.

71. As reported on BleepingComputer, another explanation for the data breach aside from Snowflake's explanation that it arose from the exploitation of customer accounts and credentials not secured by multi-factor authentication is that a threat actor stole the data after hacking into a Snowflake employee's accounts.

72. A report by Israeli cybersecurity firm Hudson Rock that has since been taken down but whose contents are reproduced in the BleepingComputer article states that the threat actor gained access to Snowflake's customers' data by bypassing security authentication processing by signing into a Snowflake employee's ServiceNow account using stolen credentials.

73. The ServiceNow account appears to have been integrated into Snowflake's IT's environment and signing into this account allowed the hacker to bypass security protections from Snowflake's single sign-on provider Okta. The threat actor(s) then generated session tokens to infiltrate data belonging to Snowflake customers.

74. The Hudson Rock report further stated that a Snowflake employee was infected by a Lumma-type Infostealer in October. The malware stole the employee's corporate credentials to Snowflake infrastructure.

75. The veracity of this account of the data breach is disputed, but Live Nation-Ticketmaster and Snowflake's individual and collective negligence is nevertheless established.

> Live Nation-Ticketmaster negligently assessed and consequently negligently or fraudulently misrepresented the safety and security of its third-party cloud-based data storage and protection service provider, the Defendant Snowflake;
>
> Live Nation-Ticketmaster selected Snowflake as its vendor and provider of third-party public cloud data storage services despite the

vulnerabilities of Snowflake's IT environment and the ability of ServiceNow credentials to be used to bypass Snowflake's singlefactor authentication;

Snowflake was negligent in failing to prevent users logging into its IT environment using ServiceNow from bypassing its single-factor authorization feature provided by Okta and thereby accessing the personal and private information of its customers' own customers.

76. Live Nation-Ticketmaster's own negligence in failing to effectively protect Class Members' data is compounded by their failure to provide timely notice of the data-compromising cyber-incident to Class Members. Plaintiff and Class Members were not notified prior to Live Nation's SEC filing dated May 31, 2024 of the cyber incident's occurrence, nature, or extent, or as to whether their private and personal information had been compromised.

77. The April-May 2024 data breach affecting the personal and private information of Ticketmaster users and customers stored on Snowflake's cloud-based environment is not an isolated incident.

78. As reported by the BBC in an article the same day Live Nation's SEC filing was made public, May 31, 2024, the ShinyHunters hacking group announced having stolen and compromised the personal and private information of at least 30 million customers and employees of European bank Santander, who was also client of Snowflake for public cloud data-storage and protection services.

79. The BBC also reports that the hacking and data theft incidents compromising the private and personal customer information of Ticketmaster and Santander are part of a broader hacking campaign against Snowflake, Inc., which provides third-party cloud-based storage services for several large companies. Additional hacking incidents are expected to be revealed in the near future.

80. The Live Nation-Ticketmaster Defendants are subject to Canadian federal and provincial legislation and are required to report breaches involving Canadian customers' data when a breach poses a real risk of significant harm to an identifiable individual.

81. The Live Nation-Ticketmaster Defendants are subject to British Columbia's private sector *Personal Information Protection Act* ("*PIPA*") in respect of the data it collects and generates from consumers and account-holders resident across Canada on the Ticketmaster.ca website and app. This includes its express responsibility "for protecting the personal information in its custody or under its control" at any given time (s. 34).

82. The Live Nation-Ticketmaster Defendants were and are subject to the federal *PIPEDA* insofar as it applies to organizations who disclose personal information collected or used in British Columbia to entities outside the province for consideration (s. 30).

83. This necessarily extends to any disclosure of said personal information by the Ticketmaster Canada Defendants as part of a transfer to one or more of the Ticketmaster family or companies, and/or Snowflake, Inc. Sections 10.1(1) and (3) of *PIPEDA* require Live Nation-Ticketmaster to report any breach of security safeguards involving personal information under their control if it is reasonable in the circumstances to believe that the breach of security safeguards creates a real risk of significant harm to an individual.

84. As reported by Global News, on May 31, 2024, the Privacy Commissioner of Canada, Philippe Dufresne, indicated being "aware of media reports" concerning the data theft incident but stated that his office "has not yet been notified of Canadian customer data being involved in the breach." The Commissioner did, however, state that he has contacted Ticketmaster to "obtain more information and determine next steps."

85. On June 1, 2024, Australia's Cyber Security Centre, part of the Australian Signals Directorate, issued a "high alert" in respect of the data theft incident, also stating that it "is tracking increased cyber threat activity relating to Snowflake customer environments"

and that it "is aware of successful compromises of several companies utilizing Snowflake environments."

86. The April-May 2024 data breach is not first data breach involving Live Nation and Ticketmaster and the vast amount of private and personal customer information it holds.

87. As reported by the BBC, in June 2018, Ticketmaster notified 40,000 UK customers of a hack caused by malicious software on third-party customer support software it had contracted from Inbenta Technologies and stated that customers who had purchased tickets between February and 23 June 2018 may have had their personal and payment information compromised. Ticketmaster also offered notified customers a free 12-month subscription to an identity monitoring service.

88. The May 2024 data theft incident was announced to have occurred by Live Nation a mere few days after the US Department of Justice announced on May 20, 2024 that it had launched a civil antitrust lawsuit with 30 state and district attorneys generals against Live Nation-Ticketmaster for "monopolization and other unlawful conduct that thwarts competition in markets across the live entertainment industry" in the United States. This conduct is alleged to violate section 2 of the *Sherman Act*, the federal antitrust statute.

89. The US DOJ Press Release quotes US Attorney General Merrick Garland as saying: "It is time to break up Live Nation Ticketmaster."

90. On July 31, 2024, the Office of the Privacy Commissioner of Canada announced that it launched an investigation into the Ticketmaster data breach in response to a complaint registered by a member of the public. The investigation:

> will assess Ticketmaster's compliance with the federal private-sector privacy law, the *Personal Information Protection and Electronic Documents Act* (PIPEDA). It will examine the company's practices with respect to security safeguards and whether the company complied with breach notification requirements.

[...]

Ticketmaster holds the personal information of millions of Canadians. The investigation will allow us to understand why this cyber incident happened and what must be done to address this situation and prevent it from happening again.

PART 2 – RELIEF SOUGHT

91. An order that the Plaintiff is appointed as Class Representative;

92. An order certifying this action as a class proceeding under the *Class Proceedings Act,* RSBC 1996, c 50;

93. A declaration that the defendants owed a duty of care to the plaintiff and the Class and breached the standard of care owed to them;

94. A declaration that the defendants are jointly and severally liable with the hacker pursuant to the negligence statutes of British Columbia, Saskatchewan, Manitoba, and Newfoundland and Labrador;

95. Statutory damages for breach of s. 1 of the *Privacy Act*, RSBC 1996, c 373 and analogous provincial and territorial legislation;

96. A declaration that the Defendants breached their contract with each Class member;

97. Assessment of aggregate damages;

98. Punitive damages;

99. Pre- and post-judgment interest under the *Court Interest Act*, RSBC 1996, c. 79;

100. Such further and other relief as this Honourable Court may deem just.

PART 3 – LEGAL BASIS

101. The Plaintiff pleads and relies on common law causes of action and statutory causes of action recognized in British Columbia and/or in the other Provinces and Territories in which Class Members reside.

102. The Plaintiff pleads and relies on the *Class Proceedings Act*, the *Privacy Act*, and the *Business Practices and Consumer Protection Act*.

Negligence

103. The Defendants owed a duty of care to the Class Members in their collection, use and storage of Class Members' personal information, to keep the personal information confidential and secure, and to ensure that it would not be lost, disseminated, or disclosed to unauthorized persons or entities.

104. Specifically, the Defendants owed Class Members a duty of care to take reasonable steps to establish, maintain and enforce appropriate security safeguards against a cyberattack and/or limit the exposure of the Class's personal information in the case of a successful cyberattack.

105. There was a sufficient degree of proximity between the Class Members and the Defendants to establish a duty of care:

a) it was reasonable for the Plaintiffs and other Class Members to expect that the Defendants had implemented appropriate security safeguards and encryption of their personal and private information against a cyberattack and to limit the exposure of their personal and private information in case of a cyberattack;

b) it was reasonably foreseeable that, if a cyberattack resulted in the extraction, theft or exfiltration of the Class Members' personal and private information, the Class Members would sustain damages;

c) it was reasonably foreseeable to the Defendants that, if they failed to take appropriate security measures to protect the personal and private information, there was a risk that the Class Members' privacy would be breached, because

of the sensitive nature of the data stored and the increasing number of cyberattacks targeted toward companies which collect and store such sensitive information, and because Ticketmaster had previously encountered a cyber attack compromising the personal information of users and customers in June 2018;

d) the Class Members were vulnerable to the Defendants, and relied on them to take appropriate security measures to protect their personal and private information;

e) the Defendants, through their Terms of Service and their Privacy Policy, promised and undertook to take appropriate measures to protect the Class Members' personal and private information;

f) there is a sufficient degree of proximity between the Class Members and the Defendants because the Class Members are, or were, customers of the Defendants and purchased tickets on the Ticketmaster website(s) and/or app(s);

g) the Defendants were required by sections 4.1, 4.5 and 4.7 of Schedule 1 to the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 (the "PIPEDA"), to implement safeguards appropriate to the sensitivity of the information stored on their network; and

h) there was a contractual relationship between the Class Members and the Defendants.

106. The Defendants were negligent and failed in their duty to implement an appropriate standard of care in establishing adequate security safeguards in collecting, managing, storing, and/or securing the Class Members' Personal Information. Without limiting the generality of the foregoing, the particulars of negligence include

a) failing to handle the collection, retention, security and disclosure of the Class Members' Personal Information in accordance with the Privacy Policy;

b) failing to designate, hire and/or properly train and/or supervise individuals responsible and accountable for network security management, including compliance internal policies and legislation in its collection, storage, protection and destruction of the Personal Information, contrary to s. 4.1 of Schedule 1 to the *PIPEDA*;

c) allowing the Personal Information to be used and disclosed for purposes other than those for which it was collected, contrary to s. 4.5 of Schedule I to the *PIPEDA*;

d) failing to implement appropriate physical, organizational and technological safeguards to protect the Personal Information against loss, theft, unauthorized access, disclosure, copying, use, and/or modification, as particularized in contrary to s. 4.7 of Schedule 1 to the *PIPEDA*;

e) failing to keep Class Members' Personal Information secure and confidential;

f) storing the Class Members' Personal Information on an unreliable server(s) vulnerable to cyber attacks;

g) failing to implement any, or adequate, cyber-security measures, programs, safeguards and internal controls to protect the Personal Information and health records of the Class Members from loss, theft, unauthorized access, unauthorized use, unauthorized duplication and/or unauthorized disclosure,

h) failing to protect the Class Members' Personal Information from compromise, disclosure, and/or theft;

i) failing to take steps to prevent the Class Members' Personal Information from being disseminated or disclosed to the public;

j) failing to immediately notify Class Members of the breach and failing to provide sufficient information to allow the Class Members to understand the significance of the breach to them and to take steps, if any are possible, to reduce the risk of harm or mitigate the harm that could result from the breach.

107. As a result of the Defendants' negligence, the hacker(s) were able to gain access to the Class Members' sensitive personal and private information, resulting in the Class Members sustaining damages.

108. The Plaintiffs state that as a result of the Defendants' negligence, the Defendants are jointly and severally liable with the hacker for the intentional privacy torts as pleaded below. The Plaintiffs plead and rely on the *Negligence Act*, RSBC 1996, c. 333, s. 4(2)(a).

Breach of Contract / Contractual Warranties

109. The Plaintiff and every Class Member entered into a contract with the Live Nation-Ticketmaster Defendants when using their services. In exchange for paying ticket prices using their credit and/or debit card information tied to their personal identity and agreeing that the Live Nation-Ticketmaster Defendant could collect, use and store the Class

Member's Personal Information, customers were provided with tickets to events and other ancillary services and benefits connected thereto.

110. The relevant provisions of the Live Nation-Ticketmaster Defendants' Privacy Policy are pleaded in the Facts Section of the Claim.

111. The Live Nation-Ticketmaster Defendants had a contractual obligation to maintain confidentiality over the personal and private information they collected from the Plaintiffs and the Class Members, which they stored in Snowflake's databases, to secure aforesaid personal and private information against such risks as unauthorized access, collection, use, disclosure and copying, and to permanently delete and destroy outdated customer personal and private information, in accordance with its own privacy policies, applicable laws and industry standards. The Live Nation-Ticketmaster Defendants breached their contracts with the Plaintiffs and the Class Members by failing to comply with the terms of service and privacy policy resulting in unauthorized access.

112. The Live Nation-Ticketmaster Defendants warranted to the Plaintiffs and the Class Members, through their Privacy Policy that they were committed to protecting their privacy. The Defendants breached their warranty by failing to take reasonable efforts to protect the Class Members' personal and private information, resulting in unauthorized access.

113. The Defendants had an express or alternatively implied contractual obligation to comply with applicable privacy legislation including PIPEDA and to manage private information in a manner that was consistent with the principles that are reflected in such legislation.

114. By promising to comply with the applicable privacy legislation in their Privacy Policy and Agreement, the Defendants also incorporated the legislation into the contract and have therefore breached their contract with the Class Members by failing to comply with the applicable privacy legislation.

Breach of Contractual Duties of Honesty, Good Faith & Fair Dealing

115. The Live Nation-Ticketmaster Defendants had a contractual duty to act honestly and in good faith. At a minimum, the Live Nation-Ticketmaster Defendants were required to make reasonable efforts to maintain confidentiality over the personal and private information they collected from the Plaintiffs and Class Members and stored on Snowflake's third-party public cloud databases and to secure said information against risks of unauthorized access, collection, use, disclosure and copying, including by ensuring the reliability and security of said cloud databases.

116. The Live Nation-Ticketmaster Defendants represented through their Privacy Policy that they had established reasonable security safeguards for the personal and private information of the Plaintiffs and Class Members. The Live Nation-Ticketmaster Defendants knew or ought to have known that the personal and private information provided by Class Members was highly sensitive and that the Class Members relied on them to secure said information.

117. The Live Nation-Ticketmaster Defendants breached their duties of honesty, and good faith and fair dealing by failing to take reasonable steps to secure the information stored on its network, when it promised and made assurances that it had done so.

Breach of Confidence

118. The Class Members were required to provide personal and private information to the Defendants in exchange for services, which was then stored electronically on its internal network.

119. The Class Members' personal and private information was confidential, sensitive and not public knowledge, exhibiting the necessary qualities to require confidence.

120. The Class Members' personal and private information was imparted to the Defendants in circumstances in which an obligation of confidence arose, and in which the Plaintiffs and

the Class Members could have reasonably expected their sensitive information to be protected and secured.

121. The Defendants made unauthorized use of the Class Members' personal and private information by failing to make reasonable efforts to maintain its confidentiality, secure aforesaid information against such risks as unauthorized access, collection, use, disclosure and copying, and to permanently delete and destroy outdated information, in accordance with the Defendants' own privacy policies, applicable laws and industry standards. The Defendants' aforesaid unauthorized use violated the PIPEDA, including sections 4.1, 4.5 and 4.7 of Schedule 1 to that legislation.

122. The Defendants' misuse resulted in unauthorized access and public disclosure of the personal and private information to the detriment of the Class Members. The Defendants are therefore liable for the tort of breach of confidence.

Breach of Applicable Consumer Protection Legislation

123. The Live Nation-Ticketmaster Defendants are subject to the provisions of the British Columbia *Business Practices and Consumer Protection Act* because it entered into consumer contracts with individuals resident in British Columbia. The Plaintiff and British Columbia Class Members each entered into consumer agreements or conducted consumer transactions with the Live Nation-Ticketmaster Defendants.

124. The Live Nation-Ticketmaster Defendants are subject to the provisions of Ontario's *Consumer Protection Act* because it entered into consumer contracts with individuals resident in Ontario. By misrepresenting to the Plaintiff and Class Members that their Personal Information would be secure, the said Defendants breached ss. 14(1) and 14(2) of Ontario's *Consumer Protection Act*.

125. Similarly, Class Members resident in other provinces entered into consumer contracts with the Live Nation-Ticketmaster Defendants pursuant to the consumer protection legislation applicable in their respective provinces.

126. The Live Nation-Ticketmaster Defendants are subject to the obligations of the Applicable Consumer Protection Legislation, which prohibits persons who enter into agreements or conduct transactions with consumers from engaging in prohibited practices.

127. The Live Nation-Ticketmaster Defendants' failure to take reasonable measures to secure the personal and private information and data constitutes a prohibited practice because Live Nation-Ticketmaster Defendants made false and misleading representations to the Class Members in relation to their security measures. Without limiting the generality of the foregoing, the particulars of which are as follows:

> (a) at the times that the Class Members used the Ticketmaster website(s) and/or app(s), the Live Nation-Ticketmaster Defendants represented that they would comply with their own privacy policy and PIPEDA, and protect the Class Members' privacy, including their personal and private information and financial information contained in their Accounts; and
>
> (b) the Live Nation-Ticketmaster Defendants failed to disclose to Class Members that their security measures were inadequate to secure the privacy of their personal and private information and the equivalent provisions of the other Applicable Consumer Protection Legislation, for engaging in unfair and/or unconscionable acts or practices. The Live Nation-Ticketmaster Defendants are therefore liable to the Plaintiffs and Class Members for the damages suffered as a result of the false, misleading and deceptive representations made to them.

Damages

128. The Plaintiff claims on his own behalf and of Class Members non-pecuniary damages on an aggregate basis flowing from the stress and anxiety arising from the data breach of his and Class Members' highly sensitive personal information that exceed the ordinary troubles and inconveniences of life.

129. The Plaintiff also claims on his own behalf and of Class Members, (a) the recovery of the entirety of monies spent to purchase credit monitoring and identity theft protection from Equifax; (b) the costs to purchase credit monitoring and identity theft protection beyond the time period offered free by the Defendants (i.e. 1 year) from Equifax and/or TransUnion – the whole to palliate the inadequate, partial, ineffective and temporary credit monitoring protection from TransUnion that was offered by the Defendants to Plaintiff and Class Members; (c) the costs to purchase data removal services to have personal information removed from the dark web; and (d) the costs to purchase protection against malicious links (phishing, etc.) sent by email and SMS.

130. Additionally, the Class Members have suffered or will likely suffer further damages from identity theft and/or fraud in the event that the personal and private information was or becomes publicly available on the internet and may be downloaded and used for criminal purposes.

131. There is a real and substantial risk that the Personal Information may be released on the internet or used in the future for criminal purposes, thereby causing the Class Members to suffer damages.

132. The Plaintiff also claims for the time and effort expended by Class Members trying to avoid suffering injury or correcting injury already suffered, such as fraud and identity theft.

Punitive Damages

133. The Live Nation-Ticketmaster Defendants' misconduct as described above, was malicious, oppressive and highhanded, and markedly departed from ordinary standards of decent behaviour. T he Defendants egregiously violated the trust and security of Class Members.

134. The Defendants' actions offend the moral standards of the community and warrant this Honourable Court's condemnation. An award of punitive damages should therefore be ordered.

Joint and Several Liability

135. The Defendants are jointly and severally liable for the acts of each of them.

Service on Out-of-Province Defendants

136. The Plaintiff and Class Members have the right to serve this Notice of Civil Claim on the Defendants pursuant to the *Court Jurisdiction and Proceedings Transfer Act*, SBC 2003, c 28, s 10 (CJPTA), because there is a real and substantial connection between British Columbia and the facts on which this proceeding is based.

    a. a tort committed in British Columbia (CJPTA, s. 10(g)); and

    b. a business carried on in British Columbia (CJPTA, s. 10(h))

137. An action under the *Privacy Act* must be determined in the Supreme Court of British Columbia (*Privacy Act*, s. 4).

Relevant Statutes

138. The Plaintiffs plead and rely upon the *Class Proceedings Act*, *PIPEDA*, the *Negligence Act*, the *Business Practices and Consumer Protection Act*, SBC 2004, c. 2, the *Privacy Act*, RSBC 1996 c. 373, and applicable analogous provincial and territorial legislation, including but not limited to applicable Consumer Protection Legislation.

Plaintiff's address for service:

Consumer Law Group Professional Corporation
150 Elgin Street, 10th Floor
Ottawa, ON K2P 1L4

Fax number for service: (613) 627-4893

Email address for service:
jorenstein@clg.org
ldavid@clg.org

The address of the registry is:

800 Smithe Street
Vancouver, BC
V6Z 2E1

Date: October 7, 2024.

Signature of lawyer for plaintiff
Jeff Orenstein

Rule 7-1 (1) of the Supreme Court Civil Rules states:

(1) Unless all parties of record consent or the court otherwise orders, each party of record to an action must, within 35 days after the end of the pleading period,

(a) prepare a list of documents in Form 22 that lists

(i) all documents that are or have been in the party's possession or control and that could, if available, be used by any party at trial to prove or disprove a material fact, and

(ii) all other documents to which the party intends to refer at trial, and

(b) serve the list on all parties of record.

ENDORSEMENT ON ORIGINATING PLEADING OR
PETITION FOR SERVICE OUTSIDE BRITISH COLUMBIA

The plaintiff claims the right to serve this pleading on the Defendants Snowflake Inc., Live Nation Entertainment Inc., Live Nation Canada Inc., Ticketmaster LLC, Ticketmaster Canada LP, Ticketmaster Canada Holdings ULC, Ticketmaster Canada ULC outside British Columbia on the ground that the *Court Jurisdiction and Proceedings Transfer Act*, SBC 2003, c. 28, s. 10 (*CJPTA*) applies because there is a real and substantial connection between British Columbia and the facts on which this proceeding is based. The Plaintiff and Class Members rely on the following grounds, in that this action concerns:

a. a tort committed in British Columbia (*CJPTA*, s. 10(g)); and
b. a business carried on in British Columbia (*CJPTA*, s. 10(h)).

Appendix

[*The following information is provided for data collection purposes only and is of no legal effect.*]

Part 1: CONCISE SUMMARY OF NATURE OF CLAIM:

This is a claim for damages arising out of a data security incident resulting in the theft and compromise of personal and private information of Live Nation-Ticketmaster customers and users stored on Snowflake Inc.'s public cloud servers.

Part 2: THIS CLAIM ARISES FROM THE FOLLOWING:

A personal injury arising out of:

[ ] a motor vehicle accident
[ ] medical malpractice
[x] another cause

A dispute concerning:

[ ] contaminated sites
[ ] construction defects
[ ] real property (real estate)
[ ] personal property
[x] the provision of goods or services or other general commercial matters
[ ] investment losses
[ ] the lending of money
[ ] an employment relationship
[ ] a will or other issues concerning the probate of an estate
[ ] a matter not listed here

Part 3: THIS CLAIM INVOLVES:

[x] a class action
[ ] maritime law
[ ] aboriginal law
[ ] constitutional law
[ ] conflict of laws
[ ] none of the above
[ ] do not know

Part 4:

Court Jurisdiction and Proceedings Transfer Act, SBC 2003, c 28
Court Order Interest Act, RSBC 1996, c 79
Privacy Act, RSBC 1996, c 3 73
Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5
Negligence Act, RSBC 1996, c 333
Business Practices and Consumer Protection Act, SBC 2004, c. 2.