Kyle McLean (SBN 330580)
kmclean@sirillp.com
Mason Barney (*pro hac vice*)
mbarney@sirillp.com
Tyler Bean (*pro hac vice*)
tbean@sirillp.com
SIRI & GLIMSTAD LLP
700 S. Flower Street, Suite 1000
Los Angeles, CA 90017
Tel: (213) 376-3739

Nicholas A. Migliaccio (*pro hac vice* anticipated)
nmigliaccio@classlawdc.com
Jason S. Rathod (*pro hac vice* anticipated)
jrathod@classlawdc.com
MIGLIACCIO & RATHOD LLP
412 H Street NE, Suite 302
Washington, DC, 20002
Tel: (202) 470-3520

Kristen Lake Cardoso (SBN 338762)
cardoso@kolawyers.com
Jeff Ostrow (*pro hac vice* anticipated)
ostrow@kolawyers.com
Kenneth Grunfeld (*pro hac vice* anticipated)
grunfeld@kolawyers.com
KOPELOWITIZ OSTROW P.A.
One West Las Olas Blvd., Suite 500
Fort Lauderdale, FL 33301
Tel: (954) 525-4100

Interim Class Counsel for Plaintiffs and the Proposed Class

(Additional counsel listed on signature page)

UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF CALIFORNIA
SOUTHERN DIVISION

In re: Vivendi Ticketing US LLC, d/b/a See Tickets Data Security Incident	Lead Case No. 2:23-cv-07498

1. Plaintiffs Mandi Peterson, Scott Fitzgerald, Zachary Richmond, Tom Loughead, Mason Verderame, Katie Jezierny, Rian Bodner, Christopher Aragon, and Candice Zinner, ("Plaintiffs") individually and on behalf of all others similarly situated, through their undersigned counsel, hereby allege the following against Defendant Vivendi Ticketing U.S. LLC, d/b/a/ See Tickets ("See Tickets" or "Defendant").

2. Plaintiffs bring this class action on behalf of all persons whose names, addresses, and payment card information (collectively known as "Private Information") were compromised as a result of Defendant's failure to: (i) adequately protect the Private Information of Plaintiffs and Class Members; (ii) warn Plaintiffs and Class Members of Defendant's inadequate information security practices; and (iii) effectively secure hardware containing protected Private Information using reasonable and effective security procedures free of vulnerabilities and incidents.

3. Defendant provided ticketing services for events Plaintiffs purchased event tickets for and, in making those purchases, turned their sensitive financial and other personal information over to Defendant for what they believed would be safekeeping.

4. However, in May of 2023, Defendant discovered unusual activity on its e-commerce websites. Specifically, Defendant asserts that an unauthorized third party inserted multiple instances of malicious code into certain of its checkout pages, containing Private Information, between February 28, 2023 and July 2, 2023 (the "Data Breach"). As a result, the Private Information of, upon information and belief, hundreds of thousands of individuals was compromised.

5. On or about September 6, 2023, Defendant filed a data breach notice with the Maine Attorney General's office reporting that over 323,498 customers were affected.[1]

6. Defendant did not send affected individuals breach notification letters until on or around September 6, 2023. Defendant's failure to timely notify Plaintiffs and Class Members about the Data Breach for five (5) months left them particularly vulnerable to having their Private

[1] *See* https://apps.web.maine.gov/online/aeviewer/ME/40/9507cec8-0c8c-46b7-bccf-c8baea5b2477.shtml (last visited November 27, 2023).

Information misused to their detriment.

7. Defendant's security failures enabled the hackers to steal the Private Information of Plaintiffs and members of the Class (defined below). These failures put Plaintiffs' and Class Members' Private Information and interests at serious, immediate, and ongoing risk and, additionally, caused costs and expenses to Plaintiffs and Class Members associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the Data Breach, including, as appropriate, reviewing records for fraudulent charges, cancelling and reissuing payment cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, initiating and monitoring credit freezes, and the stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach.

8. Plaintiffs and Class Members have already experienced misuse of their compromised Private Information, including fraudulent charges to their payment cards and attempts by criminals to open accounts in their names.

9. Thus, Plaintiffs and Class Members have suffered ascertainable losses in the form of actual fraudulent misuse of their compromised Private Information, the loss of the benefit of their bargain made with See Tickets, out-of-pocket expenses dealing with and mitigating the direct impact of the Data Breach on their lives, and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

10. Plaintiffs greatly value their privacy and would not have chosen to do business with Defendant if they had known Defendant would negligently maintain their Private Information as it did.

11. The Data Breach was caused and enabled by Defendant's violation of its obligations to abide by best practices, industry standards, and federal and state laws concerning the security of individuals' Private Information. Defendant knew or should have known that its failure to take reasonable security measures— which could have prevented or mitigated the Data Breach that occurred— left its customers' Private Information vulnerable to identity theft, financial loss, and other associated harms.

12. Defendant and its employees failed to properly monitor the computer network and systems that housed the Private Information. Had Defendant properly monitored its website, it would have discovered the Data Breach sooner.

13. Importantly, this is the second major data breach that See Tickets has reported in less than a year's time. In October of 2022, Defendant reported a different data breach that impacted over 400,000 customers' payment card data.[2]

14. The potential for improper disclosure of Plaintiffs' and Class Members' Private Information was a known risk to Defendant, especially given the previously reported data breach, and thus Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

15. Defendant and its employees failed to properly monitor the computer network and systems that housed the Private Information. Had Defendant properly monitored its website, it would have discovered the Data Breach sooner.

16. Plaintiffs' and Class Members' identities are now at risk because of Defendant's negligent conduct, especially in light of the fraudulent misuse that has already occurred.

17. Accordingly, Plaintiffs assert claims for negligence, breach of implied contract, unjust enrichment/quasi-contract, breach of confidence, violation of the New York General Business Law, N.Y. Gen. Bus. Law § 349, *et seq.*, violation of the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 Ill. Comp. Stat. 505/1, *et seq.*, violation of the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. 510/2, *et seq.*, violation of the Washington Consumer Protection Act, Wash. Rev. Code Ann. § 19.86.020, *et seq.*, violation of the California Consumer Privacy Act, Cal. Civil Code § 1798.100, *et seq*., violation of the California Consumer Legal Remedies Act, Cal. Civil Code § 1750, *et seq.*, violation of the California Constitution's right to privacy (Cal. Const., art. I, § 1), violation of the Michigan Consumer Protection Act, Mich. Comp. Laws Ann. §§ 445.903 *et seq*, violation of the Ohio Consumer Sales Practices Act, Ohio Rev. Code §§ 1345.01 *et seq*, and the Ohio Deceptive Trade

[2] *See id.*

Practices Act, Ohio Rev. Code §§ 4165.01 *et seq.*

18. Plaintiffs also seek injunctive relief, monetary damages, statutory damages, and all other relief as authorized in equity or by law.

PARTIES

A. PLAINTIFF MANDI PETERSON

19. Plaintiff Mandi Peterson is, and all times mentioned herein was, a resident and citizen of Michigan and brings this action in her individual capacity and on behalf of all others similarly situated.

20. Ms. Peterson used Defendant's ticketing services in the course of which Defendant collected, maintained, and controlled her Private Information.

21. In maintaining Ms. Peterson's Private Information, Defendant expressly and impliedly promised to safeguard it. Defendant, however, did not implement proper, industry-standard safeguards to protect her Private Information, leading to its exposure and exfiltration by cybercriminals, who stole the Private Information at issue with the intent to sell it and/or fraudulently misuse it for their own gain.

22. Ms. Peterson's Private Information, including her sensitive payment card data, was compromised as a direct and proximate result of the Data Breach and subsequently misused. Specifically, the payment card she used to make purchases on Defendant's website was used to make fraudulent purchases totaling more than $1,000.00.

23. Based on this fraudulent activity, Ms. Peterson was forced to spend significant time obtaining new payment cards, cancelling many automatic payments tied to the compromised card, and reconfiguring automatic payments on her new payment card. Given the fraudulent misuse of her Private Information that occurred, Ms. Peterson was also forced to purchase advanced security credit monitoring services through Norton Lifelock, which costs her roughly $40.00/month.

24. As a direct and proximate result of Defendant's conduct, Ms. Peterson and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

B. PLAINTIFF SCOTT FITZGERALD

25. Plaintiff Scott Fitzgerald is, and all times mentioned herein was, a resident and citizen of New York and brings this action in his individual capacity and on behalf of all others similarly situated.

26. Mr. Fitzgerald used Defendant's ticketing services in the course of which Defendant collected, maintained, and controlled his Private Information.

27. In maintaining Mr. Fitzgerald's Private Information, Defendant expressly and impliedly promised to safeguard it. Defendant, however, did not implement proper, industry-standard safeguards to protect his Private Information, leading to its exposure and exfiltration by cybercriminals, who stole the Private Information at issue with the intent to sell it and/or fraudulently misuse it for their own gain.

28. After the Data Breach, Mr. Fitzgerald was notified that his phone number was listed on the dark web. He has also received a large influx of cryptic text messages from unfamiliar numbers since the Data Breach.

29. As a direct and proximate result of Defendant's conduct, Mr. Fitzgerald and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

C. PLAINTIFF ZACHARY RICHMOND

30. Plaintiff Zachary Richmond is, and at all times mentioned herein was, a resident and citizen of Illinois and brings this action in his individual capacity and on behalf of all others similarly situated.

31. Mr. Richmond has been a See Tickets customer for at least four years. He has a current account and last made a purchase in March of 2023. He used Defendant's ticketing services, during the course of which Defendant collected, maintained, and controlled his Private Information.

32. In maintaining Mr. Richmond's Private Information, Defendant expressly and impliedly promised to safeguard it. Defendant, however, did not implement proper, industry-standard safeguards to protect his Private Information, leading to its exposure and exfiltration by

cybercriminals who stole the Private Information at issue with the intent to sell it and/or fraudulently misuse it for their own gain.

33. Mr. Richmond's Private Information, including his sensitive payment card data, was compromised as a direct and proximate result of the Data Breach and subsequently misused. Specifically, the payment card Plaintiff used to make purchases on Defendant's website was used to make three different fraudulent purchases adding up to hundreds of dollars.

34. Based on this fraudulent activity, Mr. Richmond was forced to spend significant time obtaining new payment cards.

35. Mr. Richmond has also received a large influx of cryptic emails since the Data Breach.

36. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence. Further, as the sole provider of tickets to events that Plaintiff plans to attend in the future, he knows he will be required to continue to use See Tickets in the future for ticketing needs.

37. As a direct and proximate result of Defendant's conduct, Mr. Richmond and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

D. PLAINTIFF TOM LOUGHEAD

37. Plaintiff Tom Loughead is, and all times mentioned herein was, a resident and citizen of Washington and brings this action in his individual capacity and on behalf of all others similarly situated.

38. Mr. Loughead used Defendant's ticketing services in the course of which Defendant collected, maintained, and controlled his Private Information.

39. In maintaining Mr. Loughead's Private Information, Defendant expressly and impliedly promised to safeguard it. Defendant, however, did not implement proper, industry-standard safeguards to protect his Private Information, leading to its exposure and exfiltration by cybercriminals, who stole the Private Information at issue with the intent to sell it and/or

fraudulently misuse it for their own gain.

40. As a direct and proximate result of Defendant's conduct, Mr. Loughead and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

E. PLAINTIFF MASON VERDERAME

41. Plaintiff Mason Verderame is, and all times mentioned herein was, a resident and citizen of Pennsylvania and brings this action in his individual capacity and on behalf of all others similarly situated.

42. Mr. Verderame used Defendant's ticketing services in the course of which Defendant collected, maintained, and controlled his Private Information.

43. In maintaining Mr. Verderame's Private Information, Defendant expressly and impliedly promised to safeguard it. Defendant, however, did not implement proper, industry-standard safeguards to protect his Private Information, leading to its exposure and exfiltration by cybercriminals, who stole the Private Information at issue with the intent to sell it and/or fraudulently misuse it for their own gain.

44. As a direct and proximate result of Defendant's conduct, Mr. Verderame and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

F PLAINTIFF KATIE JEZIERNY

45. Plaintiff Katie Jezierny is, and all times mentioned herein was, a resident and citizen of Illinois and brings this action in her individual capacity and on behalf of all others similarly situated.

46. Ms. Jezierny used Defendant's ticketing services in the course of which Defendant collected, maintained, and controlled her Private Information.

47. In maintaining Ms. Jezierny's Private Information, Defendant expressly and impliedly promised to safeguard it. Defendant, however, did not implement proper, industry-standard safeguards to protect her Private Information, leading to its exposure and exfiltration by cybercriminals, who stole the Private Information at issue with the intent to sell it and/or

fraudulently misuse it for their own gain.

48. Ms. Jezierny's Private Information, including her sensitive payment card data, was compromised as a direct and proximate result of the Data Breach and subsequently misused. Specifically, a criminal used her name and payment card information to withdraw $300 at her bank branch. On a second occasion, the criminal attempted to withdraw funds but was thwarted by bank security.

49. Based on this fraudulent activity, Ms. Jezierny was forced to spend significant time filing a police report, obtaining new payment cards, cancelling many automatic payments tied to the compromised card, and reconfiguring automatic payments on her new payment card.

50. As a direct and proximate result of Defendant's conduct, Ms. Jezierny and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

G. PLAINTIFF RIAN BODNER

51. Plaintiff Rian Bodner is, and all times mentioned herein was, a resident and citizen of California and brings this action in his individual capacity and on behalf of all others similarly situated.

52. Mr. Bodner used Defendant's ticketing services in the course of which Defendant collected, maintained, and controlled his Private Information.

53. In maintaining Mr. Bodner's Private Information, Defendant expressly and impliedly promised to safeguard it. Defendant, however, did not implement proper, industry-standard safeguards to protect his Private Information, leading to its exposure and exfiltration by cybercriminals, who stole the Private Information at issue with the intent to sell it and/or fraudulently misuse it for their own gain.

54. Mr. Bodner's Private Information was compromised as a direct and proximate result of the Data Breach and subsequently misused. Specifically, a criminal used Mr. Bodner's name and Private Information to open two new credit cards in his name at Home Depot and Best Buy. Both cards were subsequently maxed out up to the $10,000 limit.

55. Mr. Bodner has also received a large influx of calls from unknown numbers and

cryptic emails since the Data Breach.

56. Based on this fraudulent activity, Mr. Bodner was forced to spend significant time obtaining new payment cards, cancelling many automatic payments tied to the compromised card, and reconfiguring automatic payments on his new payment card.

57. As a direct and proximate result of Defendant's conduct, Mr. Bodner and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

H. PLAINTIFF CHRISTOPHER ARAGON

58. Plaintiff Christopher Aragon is, and all times mentioned herein was, a resident and citizen of California and brings this action in his individual capacity and on behalf of all others similarly situated.

59. Mr. Aragorn used Defendant's ticketing services in the course of which Defendant collected, maintained, and controlled his Private Information.

60. In maintaining Mr. Aragorn's Private Information, Defendant expressly and impliedly promised to safeguard it. Defendant, however, did not implement proper, industry-standard safeguards to protect his Private Information, leading to its exposure and exfiltration by cybercriminals, who stole the Private Information at issue with the intent to sell it and/or fraudulently misuse it for their own gain.

61. Mr. Aragorn's Private Information was compromised as a direct and proximate result of the Data Breach and subsequently misused. Specifically, the payment card Mr. Aragorn used to make purchases on Defendant's website was used to make a fraudulent purchase in the amount of roughly $2700.

62. Based on this fraudulent activity, Mr. Aragorn was forced to spend significant time obtaining new payment cards, cancelling many automatic payments tied to the compromised card, and reconfiguring automatic payments on his new payment card.

63. As a direct and proximate result of Defendant's conduct, Mr. Aragorn and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

I. PLAINTIFF CANDICE ZINNER

64. Plaintiff Candice Zinner is, and all times mentioned herein was, a resident and citizen of Ohio and brings this action in her individual capacity and on behalf of all others similarly situated.

65. Ms. Zinner used Defendant's ticketing services in the course of which Defendant collected, maintained, and controlled her Private Information.

66. In maintaining Ms. Zinner's Private Information, Defendant expressly and impliedly promised to safeguard it. Defendant, however, did not implement proper, industry-standard safeguards to protect her Private Information, leading to its exposure and exfiltration by cybercriminals, who stole the Private Information at issue with the intent to sell it and/or fraudulently misuse it for their own gain.

67. As a direct and proximate result of Defendant's conduct, Ms. Zinner and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

J. DEFENDANT

68. Defendant Vivendi Ticketing U.S. LLC, d/b/a/ See Tickets, is a Delaware Limited Liability Corporation with its principal place of business at 6380 Wilshire Blvd, Suite 900, Los Angeles, CA 90048. Its corporate policies, including those on data privacy, are established in and emanate from the State of California.

69. Defendant is a wholly owned subsidiary of Vivendi Village, which is the live entertainment and ticketing business unit of Vivendi SE, a French mass media holding company that reported revenues of $2.76 billion in the first quarter of 2022.[3]

70. Upon information and belief, at least one member of Vivendi Ticketing U.S. LLC is not a citizen of the State of California.

[3] *See Press Release,* Vivendi (April 25, 2022), *available at* https://www.vivendi.com/wp-content/uploads/2022/04/20220425_VIV_PR_Vivendi-Q1-2022-revenues.pdf.

JURISDICTION AND VENUE

71. The Court has jurisdiction over Plaintiffs' claims under 28 U.S.C. § 1332(d)(2) ("CAFA"), because (a) there are 100 or more Class Members, (b) at least one Class Member is a citizen of a state that is diverse from Defendant's citizenship, including Plaintiffs Peterson, Fitzgerald, Richmond, Loughead, Verderame, Jezierny, and Zinner, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

72. The Court has personal jurisdiction over Defendant because its principal place of business is located, and it conducts substantial business, in this District.

73. Venue is proper in this District under 28 U.S.C. § 1391(b)(1) because Defendant maintains its principal place of business in this District and therefore reside in this District pursuant to 28 U.S.C. § 1391(c)(2). A substantial part of the events or omissions giving rise to the Class's claims also occurred in this District.

FACTUAL ALLEGATIONS

A. Defendant's Business and The Data Breach

74. Plaintiffs and Class Members were Defendant's customers. When customers make a purchase on Defendant's website, Defendant collects sensitive personal data including name, address, and payment card information.

75. In or around early September 2023, Defendant issued Notice Letters to Plaintiffs and Class Members, alerting them that their sensitive Private Information had been exposed in a Data Breach:

> **WHAT HAPPENED?** In May 2023, See Tickets became aware of unusual activity on certain of its e-commerce websites. In response, See Tickets began working with third-party cyber forensic specialists to determine the nature and extent of the compromise, secure its websites, and identify what information may have been affected and to whom it relates.
>
> In May and June of 2023, See Tickets' third-party cyber forensic specialists determined that an unauthorized party(ies) inserted multiple instances of malicious code into a number of its e-commerce checkout pages resulting in unauthorized access to, and acquisition of, certain customer payment card information used to make purchases on the websites between February 28, 2023 and July 2, 2023. Once the forensic specialists determined the dates of compromise, See Tickets took steps to identify potentially impacted customers who made purchases during this time period. This process

> completed on July 21, 2023, and See Tickets moved quickly to notify you.
>
> Please also note that as part of its response to this compromise, See Tickets took steps to implement additional safeguards to further help protect the security of payment card information on its websites. Additionally, See Tickets notified applicable regulatory bodies as required.
>
> **WHAT INFORMATION WAS INVOLVED?** Our investigation determined that the following types of your personal information were accessed and/or taken without authorization: your name, address, and payment card information.

76. Based on the Notice Letter sent to Plaintiffs and Class Members, Defendant was alerted to unusual activity indicating unauthorized access to event checkout pages on the See Tickets website in May of 2023. The unauthorized party had access to customers' Private Information starting in February 2023 and continued to have access for at least five (5) months until Defendant was able to stop the authorized access in July of 2023.

77. The delay between the initial discovery of the Breach and the belated notification to affected customers resulted in Plaintiffs and Class Members suffering harm they otherwise could have avoided had a timely disclosure been made.

78. Omitted from the Notice Letter was any explanation as to why Defendant failed to stop the unauthorized access for five months after the Data Breach began, the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these omitted details have not been explained or clarified to Plaintiffs and Class Members, who retain a vested interest in ensuring that their Private Information remains protected.

79. Thus, this "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiffs and Class Members of the Data Breach's critical facts. Without these details, Plaintiffs' and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

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

needed.

81. The Notice Letter also offered 12 months of free credit monitoring and included generic information about identity protection including steps that victims of data security incidents can take, such as examining account statements, getting a copy of a free annual credit report or implementing a fraud alert or security freeze.

82. Defendant's offer to provide 12 months of credit monitoring is woefully inadequate. Credit monitoring only alerts individuals to the misuse of their information after it happens, which might not take place until years after the Data Breach.

83. The Data Breach occurred because See Tickets failed to take reasonable measures to protect the Private Information it collected and stored. Among other things, Defendant failed to implement data security measures designed to prevent this attack, despite repeated warnings about the risk of cyberattacks and the highly publicized occurrence of many similar attacks in the recent past on other online merchants.

84. Defendant disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiffs and Class Members' Private Information was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data. As a result, the Private Information of Plaintiffs and Class Members was exfiltrated through unauthorized access by an unknown, malicious cyber hacker with the intent to fraudulently misuse it. Plaintiffs and Class Members have a continuing interest in ensuring that their compromised Information is and remains safe.

B. Defendant Failed to Comply with Industry Standards and Federal and State Law

85. As a condition of purchasing its services, Defendant requires that its customers entrust it with their highly confidential Private Information.

86. When purchasing an event ticket on the See Tickets website, customers provide:

- Email address

- Name;
- Address;
- Zip Code;
- Payment card information;
- Payment card expiration date; and
- CVV number.

87. At the time of the Data Breach, Defendant promised its customers that it would not share this sensitive information with non-Vivendi owned companies third parties.[4] Other than sharing with financial organizations to process orders, and with social media companies for marketing, the See Tickets privacy policy states:

> See Tickets will only process your data with 3rd party organizations if you have consented to hearing news and data from them. See Tickets will specify who the data will be shared with during the process of purchasing a ticket. The 3rd parties may, from time to time, send you data about the event you have purchased tickets for, as well as further data for similar shows and events.
> All 3rd party organizations must adhere to the General Data Protection Act 2018.

88. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from disclosure.

89. Defendant had obligations created by industry standards and federal and state law to keep Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

90. Plaintiffs and Class Members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligation to keep such information confidential and secure from unauthorized access.

---

[4] *See US Privacy Policy*, See Tickets, *available at* https://misc.seetickets.us/privacy/#informationwemaycollect (last visited September 10, 2023).

91. Defendant's failure to provide adequate security measures to safeguard Plaintiffs' and Class Members' Private Information is especially egregious because Defendant operates in a field which has recently been a frequent target of scammers attempting to fraudulently gain access to customers' Private Information. Cyber security professionals have consistently identified e-commerce platforms as particularly vulnerable to data breaches because of the value of the Private Information they collect and maintain.

92. The number of US data breaches surpassed 1,800 in 2021, a record high and a sixty-eight percent increase in the number of data breaches from the previous year.[5]

93. In August 2022, the Consumer Finance Protection Bureau (CFPB) published a circular on data security. The CFPB noted that "[w]idespread data breaches and cyberattacks have resulted in significant harms to consumers, including monetary loss, identity theft, significant time and money spent dealing with the impacts of the breach, and other forms of financial distress," and the circular concluded that the provision of insufficient security for consumers' data can violate the prohibition on "unfair acts or practices" in the Consumer Finance Protection Act (CFPA).[6]

94. Charged with handling sensitive Private Information, Defendant knew, or should have known, the importance of safeguarding its customers' Private Information that was entrusted to it and of the foreseeable consequences if its data security systems were breached. This includes the significant costs that would be imposed on consumers after a breach. Defendant failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

95. Despite the abundance and availability of information regarding cybersecurity

---

[5] Identity Theft Resource Center, *2021 Annual Data Breach Year-End Review*, https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/

[6] CONSUMER FIN. PROT. BUREAU, *Consumer Financial Protection Circular 2022-04: Insufficient data protection or security for sensitive consumer information* (Aug. 11, 2022), https://files.consumerfinance.gov/f/documents/cfpb_2022-04_circular_2022-08.pdf.

best practices for the e-commerce industry, Defendant chose to ignore them. These best practices were known, or should have been known by Defendant, whose failure to heed and properly implement them directly led to the Data Breach and the unlawful exposure of Private Information.

96. At a minimum, industry best practices should have been implemented by an e-commerce provider like Defendant, including but not limited to requiring customers to create strong passwords; implementing multi-layer security including firewalls and anti-malware software; encrypting data and making it unreadable without a key; updating and patching all systems with the latest security software; and better educating its employees about safe data security practices.

97. Defendant apparently did not follow these precautions because cybercriminals accessed customers' Private Information off its website for a period of at least five (5) months until Defendant was able to cease the authorized access in July of 2023.

98. Defendant was also on notice that under the FTC Act, Defendant is prohibited from engaging in "unfair or deceptive acts or practices in or affecting commerce." 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.[7]

99. Defendant is further required by the comprehensive data privacy regimes enacted by at least 12 other states to protect Plaintiffs' and Class Members' Private Information, and further, to handle any breach of the same in accordance with applicable breach notification statutes.[8]

100. The potential for improper disclosure of Plaintiffs' and Class Members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to

---

[7] *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

[8] International Association of Privacy Professionals, *Delaware Governor Signs Personal Data Privacy Act* (Sep. 12, 2023), https://iapp.org/news/a/delaware-governor-signs-personal-data-privacy-act.

take reasonable steps necessary to secure the Private Information from those risks left the Private Information in a vulnerable position.

C. Defendant Exposed Its Customers to Identify Theft, Financial Loss, and Other Harms

101. Plaintiffs and Class Members have been injured by the disclosure of their Private Information in the Data Breach.

102. The fact that Plaintiffs' and Class Members' Private Information was stolen means that it is likely for sale by cybercriminals and will be misused in additional instances in the future.

103. Private Information is a valuable commodity to identity thieves. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identify theft and financial fraud.[9] Indeed, a robust "cyber black market" exists in which criminals openly post stolen Private Information on multiple underground Internet websites, commonly referred to as the dark web.

104. The value of Plaintiffs' and Class Members' Private Information on the black market is substantial. Indeed, studies confirm that the average direct financial loss for victims of identity theft in 2014 was $1,349.[10]

105. The FTC has also recognized that consumer data is a valuable form of currency. In an FTC roundtable presentation, a former Commissioner, Pamela Jones Harbour, underscored this point:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the

---

[9] Federal Trade Commission, *Warning Signs of Identity Theft* (Sept. 2018), https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft .

[10] *See* U.S. Dep't of Justice, *Victims of Identity Theft*, OFFICE OF JUSTICE PROGRAMS: BUREAU OF JUSTICE STATISTICS 1 (Nov. 13, 2017), https://www.bjs.gov/content/pub/pdf/vit14.pdf [hereinafter *Victims of Identity Theft*].

greater potential for analysis—and profit.[11]

106. Recognizing the high value that consumers place on their Private Information, many companies now offer consumers an opportunity to sell this information.[12] The idea is to give consumers more power and control over the type of information that they share and who ultimately receives that information. And, by making the transaction transparent, consumers will make a profit from their Private Information. This business has created a new market for the sale and purchase of this valuable data.

107. The ramifications of Defendant's failure to keep its customers' Private Information secure are long-lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for six to twelve months or even longer.

108. At all relevant times, Defendant was well-aware, or reasonably should have been aware, that the Private Information it maintains is highly sensitive and could be used for wrongful purposes by third parties, such as identity theft and fraud.

109. Defendant should have been particularly aware of these risks given that its event checkout pages had previously been compromised by a malware attack between June 2019 and April 2021, exposing an unknown number of customers' Private Information.[13]

110. Had Defendant remedied the deficiencies in its security systems after the earlier breach, followed industry guidelines, and adopted security measures recommended by experts in the field, Defendant would have prevented the breach of its systems and, ultimately, the theft of

---

[11] *Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable*, FED. TRADE COMM'N (Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf.

[12] *Web's Hot New Commodity*, *supra* note 17.

[13] TechCrunch, *See Tickets Say Hackers Accessed Customers' Payment Data—Again* (Sept. 6, 2023), https://techcrunch.com/2023/09/06/see-tickets-customer-payment-cards.

consumers' Private Information.

111. The compromised Private Information in the Data Breach is of great value to hackers and thieves and can be used in a variety of ways. Information about an individual that can be logically associated with other information can be chained together, increasing its utility to criminals.

112. In addition, as technology advances, computer programs may scan the Internet with wider scope to create a mosaic of information that may be used to link information to an individual in ways that were not previously possible. This is known as the "mosaic effect."

113. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data Breaches can be the starting point for these additional targeted attacks on the victim.

114. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of "Fullz" packages.[14]

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

---

[14] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-](https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/ (last visited on May 26, 2023).

Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

116. The development of "Fullz" packages means here that the stolen PII from the Data Breach can easily be used to link and identify it to Plaintiffs' and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

117. The existence and prevalence of "Fullz" packages means that the Private Information stolen from the data breach can easily be linked to the unregulated data (like phone numbers and emails) of Plaintiffs and the other Class Members.

118. Thus, even if certain information (such as Social Security numbers) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

119. In short, the Private Information exposed is of great value to hackers and cyber criminals and the data compromised in the Data Breach can be used in a variety of unlawful manners, including opening new credit and financial accounts in users' names.

D. Plaintiffs and Class Members Suffered Damages from the Data Breach

120. Plaintiffs and the Class have been damaged by the compromise of their Private Information in the Data Breach.

121. The ramifications of Defendant's failure to keep consumers' Private Information secure are long lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to the victims may continue for years. Consumer victims of data

breaches are more likely to become victims of identity fraud.[15]

122. In addition to its obligations under state and federal laws and regulations, Defendant owed a common law duty to Plaintiffs and Class Members to protect the Private Information they entrusted to it, including to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized parties.

123. Defendant further owed and breached its duty to Plaintiffs and Class Members to implement processes and specifications that would detect a breach of its security systems in a timely manner and to timely act upon warnings and alerts, including those generated by its own security systems.

124. As a direct result of Defendant's intentional, willful, reckless, and negligent conduct which resulted in the Data Breach, unauthorized parties were able to access, acquire, view, publicize, and/or otherwise commit the identity theft and misuse of Plaintiffs' and Class Members' Private Information as detailed above, and Plaintiffs and members of the Class are at a heightened and increased substantial risk of suffering identity theft and fraud.

125. The risks associated with identity theft are serious. While some identity theft victims can resolve their problems quickly, others spend hundreds to thousands of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or be denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

126. Some of the injuries and risks associated with the loss of personal information have already manifested themselves in Plaintiffs' and other Class Members' lives. Each Plaintiffs received a cryptically written notice letter from Defendant stating that their Private Information was released, and that they should remain vigilant for fraudulent activity, with no

---

[15] *2014 LexisNexis True Cost of Fraud Study*, LEXISNEXIS (Aug. 2014), https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf.

other explanation of where this Information could have gone, or who might have access to it.

127. Plaintiffs and the Class face a substantial risk of suffering out-of-pocket fraud losses such as fraudulent charges on online accounts, credit card fraud, applications for benefits made fraudulently in their names, loans opened in their names, medical services billed in their names, government benefits fraudulently drawn in their name, and identity theft. Some Class Members have already been victims of identity theft and fraud, as alleged herein.

128. Plaintiffs and Class Members have, may have, and/or will have incurred out of pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

129. Plaintiffs and Class Members did not receive the full benefit of their bargain when using Defendant's services. Plaintiffs and Class Members were damaged in an amount at least equal to the difference in the value between the services they thought they paid for (which would have included adequate data security protection) and the services they actually received.

130. Plaintiffs and Class Members would not have obtained services from Defendant had they known that Defendant failed to properly train its employees, lacked safety controls over its computer network, and did not have proper data security practices to safeguard their Private Information from criminal theft and misuse.

131. Plaintiffs and the Class will continue to spend significant amounts of time to monitor their financial accounts for misuse. Indeed, Plaintiffs and Class Members must, as Defendant's Notice Letter instructs, "remain vigilant" and monitor their financial accounts for many years to mitigate the risk of "identity theft and fraud." [16]

132. Identity thieves can use the victim's Private Information to commit any number of frauds, such as obtaining a job, procuring housing, or even giving false information to police during an arrest. As a result, Plaintiffs and Class Members now face a real and continuing immediate risk of identity theft and other problems associated with the disclosure of their Social

[16] *See* https://apps.web.maine.gov/online/aeviewer/ME/40/9507cec8-0c8c-46b7-bccf-c8baea5b2477.shtml.

Security numbers and will need to monitor their credit for an indefinite duration. For Plaintiffs and Class Members, this risk creates unending feelings of fear and annoyance. Private information is especially valuable to identity thieves. Defendant knew or should have known this and strengthened its data systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

133. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information has diminished in value.

134. The Private Information belonging to Plaintiffs and Class Members is private and was left inadequately protected by Defendant who did not obtain Plaintiffs' or Class Members' consent to disclose such Private Information to any other person as required by applicable law and industry standards. Defendant disclosed Plaintiffs' and Class Members' Private Information as a direct result of its inadequate security measures.

135. The Data Breach was a direct and proximate result of Defendant's failure to: (a) properly safeguard and protect Plaintiffs' and Class Members' Private Information from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and common law; (b) establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiffs' and Class Members' Private Information; and (c) protect against reasonably foreseeable threats to the security or integrity of such information.

136. Defendant had the resources and the foreknowledge necessary to prevent the Data Breach, but neglected to adequately implement data security measures, despite its obligation to protect customer data.

137. Defendant did not properly train its employees, particularly its information technology department, to timely identify cyber attacks and other data security risks.

138. Had Defendant remedied the deficiencies in its data security systems and adopted security measures recommended by experts in the field, it would have prevented the intrusions into its systems and, ultimately, the theft of Plaintiffs' and Class Members' Private Information.

139. As a direct and proximate result of Defendant's wrongful actions and inactions,

Plaintiffs and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives.

140. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, twenty-nine percent spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[17]

141. Other than offering 12 months of credit monitoring, Defendant did not take any measures to assist Plaintiffs and Class Members.

142. The limited offer of credit monitoring is woefully inadequate. While some harm has already taken place, the worst is yet to come. There may be a time lag between when harm occurs versus when it is discovered, and between when Private Information is acquired and when it is used. Furthermore, identity theft monitoring only alerts someone to the fact that they have already been the victim of identity theft (*i.e.*, fraudulent acquisition and use of another person's Private Information) – it does not prevent identity theft.[18]

143. Defendant's failure to adequately protect Plaintiffs' and Class Members' Private Information has resulted in Plaintiffs and Class Members having to undertake these tasks, which require extensive amounts of time, calls, and, for many of the credit and fraud protection services, payment of money–while Defendant sits by and does nothing to assist those affected by the incident. Instead, as Defendant's notice confirms, the burden is on Plaintiffs and Class Members to discover possible fraudulent activity and identity theft and mitigate the negative

---

[17] *See* U.S. Dep't of Justice, *Victims of Identity Theft*, OFFICE OF JUSTICE PROGRAMS: BUREAU OF JUSTICE STATISTICS 1 (Nov. 13, 2017), https://www.bjs.gov/content/pub/pdf/vit14.pdf [hereinafter *Victims of Identity Theft*].

[18] *See, e.g.*, Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost*, CNBC (Nov. 30, 2017), https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-beworth-the-cost.html.

impacts arising from such fraudulent activity on their own.

144. Plaintiffs and Class Members have been damaged in several other ways as well. Plaintiffs and Class Members have been exposed to an impending, imminent, and ongoing increased risk of fraud, identity theft, and other misuse of their Private Information. Plaintiffs and Class Members must now and indefinitely closely monitor their financial and other accounts to guard against fraud. This is a burdensome and time-consuming task. Class Members have also been forced to purchase adequate credit reports, credit monitoring and other identity protection services, and have placed credit freezes and fraud alerts on their credit reports, while also spending significant time investigating and disputing fraudulent or suspicious activity on their Information.

145. The Private Information stolen in the Data Breach can be misused on its own or can be combined with personal information from other sources such as publicly available information, social media, etc. to create a package of information capable of being used to commit further identity theft. Thieves can also use the stolen Private Information to send spear-phishing emails to Class Members to trick them into revealing sensitive information. Lulled by a false sense of trust and familiarity from a seemingly valid sender (for example Wells Fargo, Amazon, or a government entity), the individual agrees to provide sensitive information requested in the email, such as login credentials, account numbers, and the like.

146. As a result of Defendant's failures to prevent the Data Breach, Plaintiffs and Class Members have suffered, will suffer, and are at increased risk of suffering:

- The compromise, publication, theft and/or unauthorized use of their Private Information;
- Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;
- Lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;

- The continued risk to their Private Information, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake appropriate measures to protect the Private Information in its possession;
- Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and
- Anxiety and distress resulting fear of misuse of their Private Information.

147. In addition to a remedy for the economic harm, Plaintiffs and Class Members maintain an undeniable interest in ensuring that their Private Information remains secure and is not subject to further misappropriation and theft.

CLASS ACTION ALLEGATIONS

148. Plaintiffs brings all counts, as set forth below, individually and as a class action, pursuant to the provisions of Rule 23 of the Federal Rules of Civil Procedure, on behalf of a "Nationwide Class," a "New York Subclass," an "Illinois Subclass," a "Washington Subclass," a "California Subclass," a "Michigan Subclass," and an "Ohio Subclass" (collectively defined as the "Class") defined as:

Nationwide Class
All persons who submitted their Private Information to Defendant and whose Private Information was compromised as a result of the data breach(es) discovered in or about July 2023.

New York Subclass
All residents of New York who submitted their Private Information to Defendant and whose Private Information was compromised as a result of the data breach(es) discovered in or about July 2023.

Illinois Subclass
All residents of Illinois who submitted their Private Information to Defendant and whose Private Information was compromised as a result of the data breach(es) discovered in or about July 2023.

Washington Subclass

All residents of Washington who submitted their Private Information to Defendant and whose Private Information was compromised as a result of the data breach(es) discovered in or about July 2023.

California Subclass
All residents of California who submitted their Private Information to Defendant and whose Private Information was compromised as a result of the data breach(es) discovered in or about July 2023.

Michigan Subclass
All residents of Michigan who submitted their Private Information to Defendant and whose Private Information was compromised as a result of the data breach(es) discovered in or about July 2023.

Ohio Subclass
All residents of Ohio who submitted their Private Information to Defendant and whose Private Information was compromised as a result of the data breach(es) discovered in or about July 2023.

149. Excluded from the Classes are Defendant and Defendant's affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

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

151. **Numerosity**—Federal Rule of Civil Procedure 23(a)(1). The members of the Class are so numerous that joinder of all Class Members would be impracticable. On information and belief, the Class has thousands of members.

152. **Commonality and Predominance**—Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3). Common questions of law and fact exist as to all members of the Class and predominate over questions affecting only individual members of the Class. Such common questions of law or fact include, inter alia:

a. Whether Defendant's data security systems prior to and during the Data

Breach complied with applicable federal and state laws and regulations including, e.g., FTCA, and the consumer protection and data security regimes of New York, Illinois, Washington, and California (as discussed below);

b. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

c. Whether Defendant properly implemented their purported security measures to protect Plaintiffs' and the Class's Private Information from unauthorized capture, dissemination, and misuse;

d. Whether Defendant took reasonable measures to determine the extent of the Data Breach after they first learned of same;

e. Whether Defendant disclosed Plaintiffs' and the Class's Private Information in violation of the understanding that the Private Information was being disclosed in confidence and should be maintained;

f. Whether Defendant's conduct constitutes breach of an implied contract;

g. Whether Defendant willfully, recklessly, or negligently failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiffs' and the Class's Private Information;

h. Whether Defendant were negligent in failing to properly secure and protect Plaintiffs' and the Class's Private Information;

i. Whether Defendant was unjustly enriched by its actions; and

j. Whether Plaintiffs and the Class are entitled to damages, injunctive relief, or other equitable relief, and the measure of such damages and relief.

153. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs, on behalf of themselves and other members of the Class. Similar or identical common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that predominate in this action.

154. **Typicality**—Federal Rule of Civil Procedure 23(a)(3). Plaintiffs' claims are typical of the claims of the other members of the Class because, among other things, all Class Members were similarly injured through Defendant's uniform misconduct described above and were thus all subject to the Data Breach alleged herein. Further, there are no defenses available to Defendant that are unique to Plaintiffs.

155. **Adequacy of Representation**—Federal Rule of Civil Procedure 23(a)(4). Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the Class they seek to represent, they have retained counsel competent and experienced in complex class action litigation, and Plaintiffs will prosecute this action vigorously. The Class's interests will be fairly and adequately protected by Plaintiffs and their counsel.

156. **Injunctive Relief**—Federal Rule of Civil Procedure 23(b)(2). Defendant has acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class under Fed. Civ. P. 23 (b)(2).

157. **Superiority**—Federal Rule of Civil Procedure 23(b)(3). 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 or other financial detriment suffered by Plaintiffs and the Class are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be impracticable for members of the Class to individually seek redress for Defendant's wrongful conduct. Even if members of the Class could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of the Nationwide Class or, Alternatively, the State Subclasses)

158. Plaintiffs fully incorporate by reference all the above paragraphs, as though fully set forth herein.

159. Upon Defendant's accepting and storing the Private Information of Plaintiffs and the Class in its computer systems and on its networks, Defendant undertook and owed a duty to Plaintiffs and the Class to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. Defendant knew that the Private Information was private and confidential and should be protected as private and confidential.

160. Defendant owed a duty of care not to subject Plaintiffs' and Class Members' Private Information to an unreasonable risk of exposure and theft because Plaintiffs and Class Members were foreseeable and probable victims of any inadequate security practices.

161. Defendant owed numerous duties to Plaintiffs and the Class, including the following:

- to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting Private Information in its possession;
- to protect Private Information using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and
- to implement processes to quickly detect a data breach and to timely act on warnings about data breaches.

162. Defendant also breached its duty to Plaintiffs and Class Members to adequately protect and safeguard Private Information by disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured Private Information. Furthering its dilatory practices, Defendant failed to provide adequate supervision and oversight of the Private Information with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted a

malicious third party to gather Plaintiffs' and Class Members' Private Information and potentially misuse it and intentionally disclose it to others without consent.

163. Defendant knew, or should have known, of the risks inherent in collecting and storing Private Information and the importance of adequate security. Defendant knew or should have known about numerous well-publicized data breaches within the medical industry.

164. Defendant knew, or should have known, that its data systems and networks did not adequately safeguard Plaintiffs' and Class Members' Private Information.

165. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

166. Defendant breached its duties to Plaintiffs and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

167. Because Defendant knew that a breach of its systems would damage thousands of its customers, including Plaintiffs and Class Members, Defendant had a duty to adequately protect its data systems and the Private Information contained thereon.

168. Defendant's duty of care to use reasonable security measures arose from of the special relationship that existed between Defendant and its customers, which is recognized by data privacy laws and regulations under the laws of 13 states.

169. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

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

171. Defendant's own conduct also created a foreseeable risk of harm to Plaintiffs and Class Members and their Private Information. Defendant's misconduct included failing to: (1) secure Plaintiffs' and Class Members' Private Information; (2) comply with industry standard

security practices; (3) implement adequate system and event monitoring; and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

172. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information, and by failing to provide timely notice of the Data Breach. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

- Failing to adequately monitor the security of Defendant's networks and systems;
- Allowing unauthorized access to Class Members' Private Information;
- Failing to detect in a timely manner that Class Members' Private Information had been compromised; and
- Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

173. Through Defendant's acts and omissions described in this Complaint, including its failure to provide adequate security and its failure to protect Plaintiffs' and Class Members' Private Information from being foreseeably captured, accessed, disseminated, stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure Plaintiffs' and Class Members' Private Information during the time it was within Defendant's possession or control.

174. Defendant's conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to failing to adequately protect the Private Information and failing to provide Plaintiffs and Class Members with timely notice that their sensitive Private Information had been compromised.

175. Neither Plaintiffs nor Class Members contributed to the Data Breach and subsequent misuse of their Private Information as described in this Complaint.

176. As a direct and proximate cause of Defendant's conduct, Plaintiffs and Class Members suffered damages as alleged above.

177. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide lifetime free credit monitoring to all Class Members.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of the Nationwide Class or, Alternatively, the State Subclasses)

178. Plaintiffs fully incorporate by reference all the above paragraphs, as though fully set forth herein.

179. Defendant solicited and invited Plaintiffs and Class Members to provide their Private Information as part of Defendant's regular business practices. When Plaintiffs and Class Members paid for Defendant's services, they provided their Private Information to Defendant.

180. In so doing, Plaintiffs and Class Members entered into implied contracts with Defendant pursuant to which Defendant agreed to safeguard and protect such information and to timely detect any breaches of their Private Information. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

181. Class Members who paid money to Defendant reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security. Defendant failed to do so.

182. Plaintiffs and Class Members would not have provided and entrusted their Private Information with Defendant in the absence of the implied contract between them and Defendant.

183. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Defendant.

184. Defendant breached the implied contracts they made with Plaintiffs and Class

Members by failing to safeguard and protect their Private Information and by failing to timely detect the Data Breach within a reasonable time.

185. As a direct and proximate result of Defendant's breaches of the implied contracts between Defendant, Plaintiffs and Class Members, Plaintiffs and Class Members sustained actual losses and damages as described in detail above.

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

COUNT III
UNJUST ENRICHMENT/QUASI-CONTRACT
(On Behalf of the Nationwide Class or, Alternatively, the State Subclasses)

187. Plaintiffs fully incorporate by reference all the above paragraphs, as though fully set forth herein.

188. Plaintiffs and Class Members conferred monetary benefits on Defendant. Specifically, they paid for services from Defendant and/or provided Defendant with their Private Information. In exchange, Plaintiffs and Class Members should have received from Defendant the services that were the subject of the transaction and should have been entitled to have Defendant protect their Private Information with adequate data security.

189. Defendant knew that Plaintiffs and Class Members conferred a benefit on it and accepted and has retained that benefit. Defendant profited from Plaintiffs' purchases and used Plaintiffs' and Class Members' Private Information for business purposes.

190. Defendant failed to secure Plaintiffs' and Class Members' Private Information and, therefore, did not provide full compensation for the benefit the Plaintiffs' and Class Members' payments and Private Information provided.

191. Defendant acquired the Private Information through inequitable means as it failed to disclose the inadequate security practices previously alleged.

192. If Plaintiffs and Class Members knew that Defendant would not secure their Private Information using adequate security, they would not have paid for Defendant's services,

nor entrusted Defendant with their Private Information.

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

194. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiffs and Class Members conferred on it.

195. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiffs and Class Members overpaid.

COUNT IV
BREACH OF CONFIDENCE
(On Behalf of the Nationwide Class or, Alternatively, the State Subclasses)

196. Plaintiffs fully incorporate by reference all the above paragraphs, as though fully set forth herein.

197. Plaintiffs and Class Members have an interest, both equitable and legal, in the Private Information that was conveyed to and collected, stored, and maintained by Defendant and which was ultimately compromised by unauthorized cybercriminals as a result of the Data Breach.

198. Defendant, in taking possession of this highly sensitive information, has a special relationship with consumers, including Plaintiffs and the Class. As a result of that special relationship, Defendant was provided with and stored private and valuable information belonging to Plaintiffs and the Class, which Defendant was required by law and industry standards to maintain in confidence.

199. Plaintiffs and the Class provided such Private Information to Defendant under both the express and/or implied agreement of Defendant to limit and/or restrict completely the use and disclosure of such Private Information without Plaintiffs' and Class Members' consent.

200. Defendant had a common law duty to maintain the confidentiality of Plaintiffs' and Class Members' Private Information.

201. Defendant owed a duty to Plaintiffs and Class Members to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting their Private

Information in its possession from being compromised, lost, stolen, accessed by, misused by, or disclosed to unauthorized persons.

202. As a result of the parties' relationship of trust, Defendant had possession and knowledge of the confidential Private Information of Plaintiffs and Class Members.

203. Plaintiffs' and Class Members' Private Information is not generally known to the public and is confidential by nature. Moreover, Plaintiffs and Class Members did not consent to nor authorize Defendant to release or disclose their Private Information to unknown criminal actors.

204. Defendant breached the duty of confidence it owed to Plaintiffs and Class Members when Plaintiffs' and Class Members' Private Information was disclosed to unknown criminal hackers by way of Defendant's own acts and omissions, as alleged herein.

205. Defendant knowingly breached its duties of confidence by failing to safeguard Plaintiffs' and Class Members' Private Information, including by, among other things: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of consumer information that resulted in the unauthorized access and compromise of the Private Information; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the Data Breach at the time it began or within a reasonable time thereafter and give adequate notice to Plaintiffs and Class Members thereof; (g) failing to follow its own privacy policies and practices published to consumers; (h) storing Private Information in an unencrypted and vulnerable manner, allowing its disclosure to hackers; and (i) making an unauthorized and unjustified disclosure and release of Plaintiffs' and Class Members' Private Information to a criminal third party.

206. But for Defendant's wrongful breach of confidence owed to Plaintiffs and Class Members, their privacy would not have been compromised and their Private Information would

not have been accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by and/or viewed by unauthorized third parties.

207. As a direct and proximate result of Defendant's breach of confidence, Plaintiffs and Class Members have suffered or will suffer injuries, including but not limited to, the following: loss of their privacy and confidentiality in their Private Information; theft of their Private Information; costs associated with the detection and prevention of fraud and unauthorized use of their Private Information; costs associated with purchasing credit monitoring and identity theft protection services; costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Defendant's Data Breach – including finding fraudulent charges, enrolling in credit monitoring and identity theft protection services, and filing reports with the police and FBI; the imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their Private Information being placed in the hands of criminals; damages to and diminution in value of their Private Information entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiffs' and Class Members' data against theft and not allow access and misuse of their data by others; continued risk of exposure to hackers and thieves of their Private Information, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' data; and/or mental anguish accompanying the loss of confidence and disclosure of their confidential Private Information.

208. Defendant breached the confidence of Plaintiffs and Class Members when it made an unauthorized release and disclosure of their confidential Private Information and, accordingly, it would be inequitable for Defendant to retain the benefits it has received at Plaintiffs' and Class Members' expense.

209. As a direct and proximate result of Defendant's breach of confidence, Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven at trial.

COUNT V
Unfair and Deceptive Trade Practices in Violation of N.Y. Gen. Bus. Law § 349, *et seq.*
(By Plaintiff Fitzgerald on Behalf of the New York Subclass)

210. Plaintiff fully incorporates by reference all the above paragraphs, as though fully set forth herein.

211. For purposes of this section only, the term "Plaintiff" refers to Plaintiff Fitzgerald, and the term "Class" refers to the New York Subclass.

212. New York General Business Law § 349 prohibits deceptive acts or practices in the conduct of any business, trade, or commerce, or in the furnishing of any service in the state of New York.

213. By reason of the conduct alleged herein, Defendant engaged in unlawful practices within the meaning of N.Y. Gen. Bus. Law § 349. The conduct alleged herein is a "business practice" within the meaning of N.Y. Gen. Bus. Law § 349, and the deception occurred within New York State.

214. Defendant stored Plaintiff's and Class Members' Private Information in Defendant's electronic databases. Defendant knew or should have known it did not employ reasonable, industry standard, and appropriate security measures that complied with all relevant regulations and would have kept Plaintiff's and Class Members' Private Information secure and prevented the loss or misuse of that Private Information. Defendant did not disclose to Plaintiff and Class Members that its data systems were not secure.

215. Plaintiff and Class Members would not have provided their Private Information if they had been told or knew that Defendant failed to maintain sufficient security thereof, and its inability to safely store Plaintiff's and Class Members' Private Information.

216. As alleged herein in this Complaint, Defendant engaged in unfair or deceptive acts or practices in the conduct of consumer transactions in violation of N.Y. Gen. Bus. Law § 349, including but not limited to:

- Representing that its services were of a particular standard or quality that it knew or should have known were of another;

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

- Failing to identify foreseeable security and privacy risks, and remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;

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

- Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and New York Subclass members' Private Information, including by implementing and maintaining reasonable security measures;

- Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and New York Subclass Members' Private Information, and;

- 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's and New York Subclass Members' Private Information, including duties imposed by the FTCA, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach.

217. Such acts by Defendant were and are deceptive acts or practices which are and/or were likely to mislead a reasonable consumer providing his or her Private Information to Defendant. Said deceptive acts and practices are material. The requests for and use of such Private Information in New York through deceptive means occurring in New York were consumer-oriented acts and thereby fall under the New York consumer fraud statute, N.Y. Gen. Bus. Law § 349.

218. In addition, Defendant's failure to secure Class Members' Private Information violated the FTCA and therefore violates N.Y. Gen. Bus. Law § 349.

219. Defendant knew or should have known that its computer systems and data

security practices were inadequate to safeguard the Private Information of Plaintiff and Class Members, deter hackers, and detect a breach within a reasonable time, and that the risk of a data breach was highly likely. Plaintiff and Class Members accordingly seek all monetary and non-monetary relief allowed by law, including actual damages, treble damages, injunctive relief, civil penalties, and attorneys' fees and costs.

220. The aforesaid conduct violated N.Y. Gen. Bus. Law § 349, in that it is a restraint on trade or commerce.

221. Defendant's violations of N.Y. Gen. Bus. Law § 349 have an impact and general importance to the public, including the people of New York. Thousands of New Yorkers have had their Private Information stored on Defendant's electronic database, many of whom have been impacted by the Data Breach.

222. As a direct and proximate result of these deceptive trade practices, Plaintiff and Class Members are entitled to judgment under N.Y. Gen. Bus. Law § 349, to enjoin further violations, to recover actual damages, to recover the costs of this action (including reasonable attorneys' fees), and such other relief as the Court deems just and proper.

223. Defendant's implied and express representations that it would adequately safeguard Plaintiff's and Class Members' Private Information constitute representations as to the particular standard, quality, or grade of services that such services did not actually have (as the services were of another, inferior quality), in violation of N.Y. Gen. Bus. Law § 349.

224. Accordingly, Plaintiff, on behalf of himself and other Class Members, brings this action under N.Y. Gen. Bus. Law § 349 to seek such injunctive relief necessary to enjoin further violations and recover costs of this action, including reasonable attorneys' fees and other costs.

COUNT VI
VIOLATION OF THE ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT
815 Ill. Comp. Stat. 505/1, *et seq.*
(By Plaintiffs Richmond and Jezierny on Behalf of the Illinois Subclass)

225. Plaintiffs fully incorporate by reference all the above paragraphs, as though fully set forth herein.

226. For purposes of this section only, the term "Plaintiffs" refers to Plaintiffs

Richmond and Jezierny.

227. In Illinois, the "Consumer Fraud and Deceptive Business Practices Act" 815 Ill. Comp. Stat. 505/1, *et seq*., prohibits "unfair methods of competition and unfair or deceptive acts or practices, including but not limited to the use or employment of any deception, fraud, false pretense, false promise, misrepresentation or the concealment, suppression or omission of any material fact, with intent that others rely upon the concealment, suppression or omission of such material fact or the use or employment of any practice described in Section 2 of the 'Uniform Deceptive Trade Practices Act' . . . ."

228. Plaintiffs and the Illinois Subclass Members were injured by Defendant's deceptive misrepresentations, concealments, and omissions, and these misrepresentations, concealments and omissions were material and deceived Plaintiffs and the Illinois Subclass. Because Plaintiffs and the Illinois Subclass Members relied on Defendant's misrepresentations, concealments, and omissions when purchasing products and services, they were injured at the time of purchase.

229. Defendant does business in Illinois and engaged in deceptive acts and practices in connection with the business in Illinois and elsewhere in the United States.

230. The products and services purchased by Plaintiffs and the Illinois Subclass Members were "consumer items" as that term is defined under the Illinois Consumer Fraud Act.

231. Defendant engaged in unfair and deceptive acts in violation of 815 Ill. Comp. Stat. 505/2 when it misrepresented and deceptively concealed, suppressed, and/or omitted the material information known to it, which has caused damage and injury to Plaintiffs and the Illinois Subclass Members. Plaintiffs and the Illinois Subclass Members were injured by Defendant's unfair and deceptive acts at the time of purchasing the products and services.

232. As alleged herein this Complaint, Defendant engaged in unfair or deceptive acts or practices in the conduct of consumer transactions, including but not limited to:

- Representing that its services were of a particular standard or quality that it knew or should have known were of another;
- Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Illinois Subclass

members' Private Information, which was a direct and proximate cause of the Data Breach;

- Failing to identify foreseeable security and privacy risks, and remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;
- Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Illinois Subclass Members' Private Information, including Duties imposed by the FTCA, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
- Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Illinois Subclass members' Private Information, including by implementing and maintaining reasonable security measures;
- Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Illinois Subclass Members' Private Information, and;
- 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 Plaintiffs' and Illinois Subclass Members' Private Information, including duties imposed by the FTCA, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach.

233. Defendant deceived its customers, which created a likelihood of confusion or of misunderstanding in violation of the Act. It knew or should have known that all consumers who purchased the products and services would be impacted by its misrepresentations and omissions.

234. These deceptive acts occurred in a course of conduct involving trade and commerce in Illinois and throughout the United States.

235. Defendant intended that Plaintiffs and the Illinois Subclass Members rely on its deceptive acts, which proximately caused actual injury and damage to Plaintiffs and the Illinois Subclass Members.

236. As a direct and proximate result of Defendant's conduct, Plaintiffs and Illinois Subclass Members have been harmed and have suffered damages including, but not limited to: (i) invasion of privacy; (ii) lost or diminished value of Private Information; (iii) lost time and

opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) and actual fraud, including an increase in spam calls, texts, and/or emails; and (vi) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

237. As a direct and proximate result of the unconscionable, unfair, and deceptive acts or practices alleged herein, Plaintiffs and Illinois Subclass Members have been damaged and are entitled to recover an order providing declaratory and injunctive relief and reasonable attorneys' fees and costs, to the extent permitted by law.

238. Plaintiffs and the Illinois Subclass Members would not have purchased, or would have paid less for, the products and services but for the material misrepresentations and omission as described in this Complaint.

COUNT VII

VIOLATION OF THE ILLINOIS UNIFORM DECEPTIVE TRADE PRACTICES ACT
815 Ill. Comp. Stat. 510/2, *et seq.*
(By Plaintiffs Richmond and Jezierny on Behalf of the Illinois Subclass)

239. Plaintiffs fully incorporate by reference all the above paragraphs, as though fully set forth herein.

240. For purposes of this section only, the term "Plaintiffs" refers to Plaintiffs Richmond and Jezierny.

241. The Illinois Deceptive Trade Practices Act ("UDTPA"), 815 Ill. Comp. Stat. 510/2, et seq., prohibits "[u]nfair methods of competition and unfair or deceptive acts or practices, including but not limited to the use or employment of any deception, fraud, false pretense, false promise, misrepresentation or the concealment, suppression or omission of any material fact, with intent that others rely upon the concealment, suppression or omission of such material fact."

242. 815 ILCS 510/2 provides in pertinent part that a "person engages in a deceptive

trade practice when, in the course of his or her business, vocation, or occupation," the person does any of the following: "(5) represents that goods or services have . . . uses, benefits or quantities that they do not have . . .; (7) represents that goods or services are of a particular standard, quality, or grade or that goods are a particular style or model, if they are of another; . . . [or] (12) engages in any other conduct which similarly creates a likelihood of confusion or misunderstanding."

243. Defendant violates this prohibition by deceiving consumers into believing they adequately protect Private Information. This creates a likelihood of confusion or of misunderstanding in violation of the Act.

244. Defendant intended that Plaintiffs and each of the other Illinois Subclass Members would reasonably rely upon the material misrepresentations and omissions concerning the true nature of the products and services.

245. Defendant's concealment, omissions, and other deceptive conduct were likely to deceive and cause misunderstanding and/or in fact caused Plaintiffs and each of the other Illinois Subclass Members to be deceived in a course of conduct involving trade and commerce in Illinois and throughout the United States.

246. Defendant's deceptive acts proximately caused actual injury and damage to Plaintiffs and the Illinois Subclass Members.

247. Plaintiffs and the Illinois Subclass Members would not have purchased, or would have paid less for, the products and services but for the material misrepresentations as described in this Complaint.

248. Defendant intended Plaintiffs and the Illinois Subclass Members to rely on its deceptive acts.

COUNT VIII
VIOLATION OF THE WASHINGTON CONSUMER PROTECTION ACT
Wash Rev. Code Ann. § 19.86.020, *et seq.*
(By Plaintiff Joughead on Behalf of the Washington Subclass)

249. Plaintiff fully incorporates by reference all the above paragraphs, as though fully set forth herein.

250. For purposes of this section only, the term "Plaintiff" refers to Plaintiff Joughead.

251. Defendant is a "person," as defined by Wash Rev. Code Ann. § 19.86.020(1).

252. Defendant advertised, offered, or sold goods or services in Washington and engaged in trade or commerce directly or indirectly affecting the people of Washington, as defined by Wash. Rev. Code Ann. § 19.86.010(2).

253. As alleged herein this Complaint, Defendant engaged in unfair or deceptive acts or practices in the conduct of consumer transactions in the conduct of trade or commerce, in violation of Wash. Rev. Code Ann. § 19.86.020, including, but not limited to:

- Representing that its services were of a particular standard or quality that it knew or should have known were of another;
- Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Washington Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;
- Failing to identify foreseeable security and privacy risks, and remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;
- Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Washington Subclass Members' Private Information, including duties imposed by the FTCA, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
- Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Washington Subclass members' Private Information, including by implementing and maintaining reasonable security measures;
- Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Washington Subclass Members' Private Information, and;
- 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's and Washington Subclass Members' Private Information, including duties imposed by the FTCA, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach.

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

255. Defendant acted intentionally, knowingly, and maliciously to violate Washington's Consumer Protection Act, and recklessly disregarded Plaintiff's and Washington Subclass Members' rights.

256. Defendant's conduct is injurious to the public interest because it violates Wash. Rev. Code Ann. § 19.86.020, violates a statute that contains a specific legislation declaration of public interest impact, and/or injured persons and had and has the capacity to injure persons. Further, its conduct affected the public interest, including, upon information and belief, the thousands of Washingtonians affected by the Data Breach.

257. As a direct and proximate result of Defendant's unfair or deceptive acts or practices, Plaintiff and Washington Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from time and expenses related to monitoring their financial accounts for fraudulent activity; and loss of value of their Private Information.

258. Plaintiff and Washington Subclass Members accordingly seek all monetary and non-monetary relief allowed by law, including actual damages, treble damages, injunctive relief, civil penalties, and attorneys' fees and costs.

COUNT IX
VIOLATION OF THE CALIFORNIA CONSTITUTION'S RIGHT TO PRIVACY
(Cal. Const., art. I, § 1)
(By Plaintiffs Aragorn and Bodner on Behalf of the California Subclass)

259. Plaintiffs fully incorporate by reference all the above paragraphs, as though fully set forth herein.

260. For purposes of this section only, the term "Plaintiffs" refers to Plaintiffs Aragorn and Bodner.

261. The California Constitution provides:

> "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty,

> acquiring, possession, and protecting property, and pursuing and obtaining safety, happiness, and privacy." (Cal. Const., art. I. § 1.)

262. Plaintiffs and the California Subclass have a legally recognized and protected privacy interest in the Private Information provided to and obtained by Defendant, including but not limited to, an interest in precluding the dissemination or misuse of this sensitive and confidential information and the misuse of this information for malicious purposes.

263. Plaintiffs and the Subclass reasonably expected Defendant would prevent the unauthorized viewing, use, manipulation, exfiltration, theft, and disclosure of their Private Information and the substantial, imminent risk of the unauthorized use thereof.

264. Defendant's conduct described herein resulted in a serious invasion of privacy of Plaintiffs and the Subclass, as the release of Private Information could highly offend a reasonable individual.

265. As a direct consequence of the actions as identified above, Plaintiffs and California Subclass Members suffered harms and losses, including but not limited to, the loss of control over use of their identity, harm to their constitutional right to privacy, lost time dedicated to the investigation and attempt to cure harm to their privacy, the need for future expenses and time dedicated to the recovery and protection of imminent future loss, and privacy injuries associated with having their sensitive Private Information disclosed.

COUNT X
VIOLATION OF THE CALIFORNIA CONSUMER PRIVACY ACT
Cal. Civ. Code § 1798.100, *et seq.*
(By Plaintiffs Aragorn and Bodner on Behalf of the California Subclass)

266. Plaintiffs fully incorporate by reference all the above paragraphs, as though fully set forth herein.

267. For purposes of this section only, the term "Plaintiffs" refers to Plaintiffs Aragorn and Bodner.

268. Defendant is a corporation organized or operated for the profit or financial benefit of its owners. Defendant collects consumers' Private Information as defined in Cal. Civ. Code § 1798.140.

269. Defendant violated § 1798.150 of the CCPA by failing to prevent Plaintiffs' and California Subclass Members' unencrypted Private Information from unauthorized access and exfiltration, theft, or disclosure as a result of Defendant's violations of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

270. Defendant has a duty to implement and maintain reasonable security procedures and practices to protect Plaintiffs' and California Subclass Members' Private Information. As detailed herein, Defendant failed to do so.

271. As a direct and proximate result of Defendant's acts, Plaintiffs' and California Subclass Members' Private Information was subject to unauthorized access and exfiltration, theft, or disclosure.

272. Plaintiffs sent a letter to Defendant on October 16, 2023 noticing Defendant of its violations of the CCPA. Defendant failed to provide class-wide relief during the subsequent 30-day period.

273. Plaintiffs and California Subclass Members seek injunctive or other equitable relief to ensure Defendant hereinafter properly safeguards customers' PII by implementing reasonable security procedures and practices. Such relief is particularly important because Defendant continues to hold customers' Private Information, including Plaintiffs' and California Subclass Members' Private Information. Plaintiff and California Subclass Members have an interest in ensuring that their Private Information is reasonably protected, and Defendant has demonstrated a pattern of failing to properly safeguard this information, as evidenced by its multiple failures to notify Plaintiffs of its data breach and to take appropriate remedial steps post breach.

274. Plaintiffs and the California Subclass seek statutory or actual damages, whichever is greater, as well as all monetary and non-monetary relief allowed by law, including actual financial losses; injunctive relief; and reasonable attorneys' fees and costs.

COUNT XI

VIOLATION OF THE CALIFORNIA CONSUMER LEGAL REMEDIES ACT

Cal. Civ. Code § 1750, *et seq.*

(By Plaintiffs Aragorn and Bodner on Behalf of the California Subclass)

275. Plaintiffs fully incorporate by reference all the above paragraphs, as though fully set forth herein.

276. For purposes of this section only, the term "Plaintiffs" refers to Plaintiffs Aragorn and Bodner.

277. Defendant is a "person," as defined by Cal. Civ. Code § 1761 and § 1770 and has provided "services" as defined by Cal. Civ. Code § 1761(b) and § 1770 and has engaged in a "transaction" as defined by Cal. Civ. Code § 1761 and § 1770.

278. As alleged herein this Complaint, Defendant engaged in unfair or deceptive acts or practices in the conduct of consumer transactions in the conduct of trade or commerce, in violation of Cal. Civ. Code § 1770, including, but not limited to:

- Representing that its services were of a particular standard or quality that it knew or should have known were of another;
- Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and California Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;
- Failing to identify foreseeable security and privacy risks, and remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;
- Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and California Subclass Members' Private Information, including duties imposed by the FTCA, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
- Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and California Subclass members' Private Information, including by implementing and maintaining reasonable security measures;
- Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and California Subclass Members' Private Information, and;

- 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 Plaintiffs' and California Subclass Members' Private Information, including duties imposed by the FTCA, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach.

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

280. Defendant acted intentionally, knowingly, and maliciously to violate California's Consumer Legal Remedies Act, and recklessly disregarded Plaintiffs' and California Subclass Members' rights.

281. Defendant's conduct is injurious to the public interest because it violates Cal. Civ. Code § 1770, violates a statute that contains a specific legislation declaration of public interest impact, and/or injured persons and had and has the capacity to injure persons. Further, its conduct affected the public interest, including, upon information and belief, the thousands of Californians affected by the Data Breach.

282. As a direct and proximate result of Defendant's unfair or deceptive acts or practices, Plaintiffs and California Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from time and expenses related to monitoring their financial accounts for fraudulent activity; and loss of value of their Private Information.

283. Plaintiffs sent a letter to Defendant on October 16, 2023 noticing Defendant of its violations of the CLRA. Defendant failed to provide class-wide relief during the subsequent 30-day period.

284. Plaintiffs and California Subclass Members accordingly seek all monetary and non-monetary relief allowed by law, including actual damages, injunctive relief, civil penalties, and attorneys' fees and costs.

COUNT XII
MICHIGAN CONSUMER PROTECTION ACT
Mich. Comp. Laws Ann. §§ 445.903 *et seq*.
(By Plaintiff Peterson on Behalf of the Michigan Subclass)

285. Plaintiffs fully incorporate by reference all the above paragraphs, as though fully set forth herein.

286. For purposes of this section only, the term "Plaintiff" refers to Plaintiff Mandi Peterson.

287. See Tickets, Plaintiff, and Michigan Subclass Members are "persons" as defined by Mich. Comp. Laws Ann. § 445.902(d).

288. See Tickets advertised, offered, or sold goods or services in Michigan and engaged in trade or commerce directly or indirectly affecting the people of Michigan, as defined by Mich. Comp. Laws Ann. § 445.902(g).

289. See Tickets engaged in unfair, unconscionable, and deceptive practices in the conduct of trade and commerce, in violation of Mich. Comp. Laws Ann. § 445.903(1), including:

- Representing that its goods and services have characteristics, uses, and benefits that they do not have;
- Representing that its goods and services are of a particular standard or quality if they are of another;
- Failing to reveal a material fact, the omission of which tends to mislead or deceive the consumer, and which fact could not reasonably be known by the consumer;
- Making a representation or statement of fact material to the transaction such that a person reasonably believes the represented or suggested state of affairs to be other than it actually is; and
- Failing to reveal facts that are material to the transaction in light of representations of fact made in a positive matter.

290. See Tickets' unfair, unconscionable, and deceptive practices include:

- Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Michigan Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;
- Failing to identify and remediate foreseeable security and privacy risks and

sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

- Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Michigan Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Michigan Identity Theft Protection Act, Mich. Comp. Laws Ann. §§ 445.72 *et seq.*, which was a direct and proximate cause of the Data Breach;

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

- Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Michigan Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Michigan Identity Theft Protection Act, Mich. Comp. Laws Ann. §§ 445.72 *et seq.*;

- Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiff's and Michigan Subclass Members' Private Information; and

- 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's and Michigan Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Michigan Identity Theft Protection Act, Mich. Comp. Laws Ann. §§ 445.72 *et seq.*

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

292. See Tickets intended to mislead Plaintiff and Michigan Subclass Members and induce them to rely on its misrepresentations and omissions.

293. See Tickets acted intentionally, knowingly, and maliciously to violate Michigan's Consumer Protection Act, and recklessly disregarded Plaintiff's and Michigan Subclass Members' rights.

294. As a direct and proximate result of See Tickets' unfair, unconscionable, and deceptive practices, Plaintiff and Michigan Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary

damages, as alleged herein, including but not limited to, 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; loss of value of their Private Information; overpayment for See Tickets' services; loss of the value of access to their Private Information; and the value of identity protection services made necessary by the Data Breach.

295. Plaintiff and Michigan Subclass Members seek all monetary and non-monetary relief allowed by law, including the greater of actual damages or $250, injunctive relief, and any other relief that is just and proper.

COUNT XIII
OHIO CONSUMER SALES PRACTICES ACT
Ohio Rev. Code §§ 1345.01 *et seq*.
(By Plaintiff Zinner on Behalf of the Ohio Subclass)

296. Plaintiffs fully incorporate by reference all the above paragraphs, as though fully set forth herein.

297. For purposes of this section only, the term "Plaintiff" refers to Plaintiff Candice Zinner.

298. Plaintiff and Ohio Subclass Members are "persons," as defined by Ohio Rev. Code § 1345.01(B).

299. See Tickets was a "supplier" engaged in "consumer transactions," as defined by Ohio Rev. Code §§ 1345.01(A) & (C).

300. See Tickets advertised, offered, or sold goods or services in Ohio and engaged in trade or commerce directly or indirectly affecting the people of Ohio.

301. See Tickets engaged in unfair and deceptive acts and practices in connection with a consumer transaction, in violation of Ohio Rev. Code § 1345.02, including:

- Representing that the subject of a transaction had approval, performance characteristics, uses, and benefits that it did not have;
- Representing that the subject of a transaction was of a particular standard or quality when they were not.

302. See Tickets engaged in unconscionable acts and practices in connection with a consumer transaction, in violation of Ohio Rev. Code § 1345.03, including:

- Knowingly taking advantage of the inability of Plaintiff and Ohio Subclass Members to reasonably protect their interest because of their ignorance of the issues discussed herein;

- Knowing at the time the consumer transaction was entered into of the inability of the consumer to receive a substantial benefit from the subject of the consumer transaction;

- Requiring the consumer to enter into a consumer transaction on terms the supplier knew were substantially one-sided in favor of the supplier; and

- Knowingly making a misleading statement of opinion on which the consumer was likely to rely to the consumer's detriment.

303. See Tickets' unfair, deceptive, and unconscionable acts and practices include:

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

- Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

- Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Ohio 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;

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

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

- Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiff's and Ohio Subclass Members' Private Information; and

- 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's and Ohio Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

304. See Tickets' representations and omissions were material because they deceived

Plaintiff and Ohio Subclass Members, and were likely to deceive other reasonable consumers, about the adequacy of See Tickets' data security and ability to protect the confidentiality of consumers' Private Information.

305. See Tickets intended to mislead Plaintiff and Ohio Subclass Members and induce them to rely on its misrepresentations and omissions.

306. See Tickets acted intentionally, knowingly, and maliciously to violate Ohio's Consumer Sales Practices Act, and recklessly disregarded Plaintiff's and Ohio Subclass Members' rights.

307. See Tickets' unfair, deceptive, and unconscionable acts and practices complained of herein affected the public interest, including the many Ohioans affected by the Data Breach.

308. As a direct and proximate result of See Tickets' unfair, deceptive, and unconscionable acts and practices, Plaintiff and Ohio Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as alleged herein, including but not limited to 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; loss of value of their Private Information; overpayment for See Tickets' services; loss of the value of access to their Private Information; and the value of identity protection services made necessary by the Data Breach.

309. Pursuant to Ohio Rev. Code § 1345.09(A), Plaintiff seeks actual economic damages and non-economic damages of up to five thousand dollars.

310. Pursuant to § Ohio Rev. Code 1345.09(D), Plaintiff seeks declaratory and injunctive relief.

311. Pursuant to Ohio Rev. Code § 1345.09(F), Plaintiff seeks an award of reasonable attorneys' fees.

COUNT XIV
OHIO DECEPTIVE TRADE PRACTICES ACT
Ohio Rev. Code §§ 4165.01 *et seq.*
(By Plaintiff Zinner on Behalf of the Ohio Subclass)

312. Plaintiffs fully incorporate by reference all the above paragraphs, as though fully

set forth herein.

313. For purposes of this section only, the term "Plaintiff" refers to Plaintiff Candice Zinner.

314. See Tickets, Plaintiff, and Ohio Subclass Members are "persons" as defined by Ohio Rev. Code § 4165.01(D).

315. See Tickets advertised, offered, or sold goods or services in Ohio and engaged in trade or commerce directly or indirectly affecting the people of Ohio.

316. See Tickets engaged in deceptive trade practices in the course of its business and vocation, in violation of Ohio Rev. Code § 4165.02, including:

- Representing that its goods and services have approval, characteristics, uses, or benefits that they do not have;
- Representing that its goods and services are of a particular standard or quality when they are of another; and
- Advertising its goods and services with intent not to sell them as advertised.

317. See Tickets' deceptive trade practices include:

- Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Ohio Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;
- Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Ohio 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;
- Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Ohio Subclass Members' Private Information, including by implementing and maintaining reasonable security measures;
- Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Ohio Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

- Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiff's and Ohio Subclass Members' Private Information; and

- 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's and Ohio Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

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

319. See Tickets intended to mislead Plaintiff and Ohio Subclass Members and induce them to rely on its misrepresentations and omissions.

320. See Tickets acted intentionally, knowingly, and maliciously to violate Ohio's Deceptive Trade Practices Act, and recklessly disregarded Plaintiff's and Ohio Subclass Members' rights.

321. As a direct and proximate result of See Tickets' deceptive trade practices, Plaintiff and Ohio Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as alleged herein, including but not limited to 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; loss of value of their Private Information; overpayment for See Tickets' services; loss of the value of access to their Private Information; and the value of identity protection services made necessary by the Data Breach.

322. Plaintiff and Ohio Subclass Members seek all monetary and non-monetary relief allowed by law, including injunctive relief, actual damages, attorneys' fees, and any other relief that is just and proper.

COUNT XV
INJUNCTIVE / DECLARATORY RELIEF
(On Behalf of the Nationwide Class)

323. Plaintiffs fully incorporate by reference all the above paragraphs, as though fully set forth herein.

324. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. The Court also has broad authority to restrain acts, such as here, that are tortious and violate the terms of the regulations described in this Complaint.

325. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's present and prospective duties to reasonably safeguard users' Private Information and whether Defendant is maintaining data security measures adequate to protect the Class Members, including Plaintiffs, from further data breaches that compromise their Private Information.

326. Plaintiffs allege that Defendant's data-security measures remain inadequate. In addition, Plaintiffs and the Class continue to suffer injury as a result of the compromise of their Private Information and remain at imminent risk that further compromises of their Private Information and fraudulent activity against them will occur in the future.

327. Pursuant to the Court's authority under the Declaratory Judgment Act, Plaintiffs ask the Court to enter a judgment declaring, among other things, the following: (i) Defendant owes a duty to secure consumers' Private Information and to timely notify consumers of a data breach under the common law and various federal and state statutes; and (ii) Defendant is in breach of these legal duties by failing to employ reasonable measures to secure consumers' Private Information in its possession and control.

328. Plaintiffs further ask the Court to issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry standards to protect consumers' Private Information from future data breaches.

329. If an injunction is not issued, the Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Defendant. The risk of another such breach is real, immediate, and substantial. If another breach at Defendant occurs, the Class Members will not have an adequate remedy at law because many of the resulting injuries would not be readily quantifiable and Class Members will be forced to bring multiple lawsuits to rectify the same misconduct.

330. The hardship to the Class Members if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Among other things, if a similar data breach occurs again due to the repeated misconduct of Defendant, the Class Members will likely be subjected to substantial hacking and phishing attempts, fraud, and other instances of the misuse of their Private Information, in addition to the damages already suffered. On the other hand, the cost to Defendant of complying with an injunction by employing better and more reasonable prospective data security measures is relatively minimal, and Defendant has pre-existing legal obligations to employ such measures.

331. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing additional data breaches at Defendant, thus eliminating the additional injuries that would result to the Class Members and the consumers whose personal and confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for judgment as follows:

a. For an order certifying the proposed Classes and appointing Plaintiffs and their counsel to represent the Classes;

b. For an order awarding Plaintiffs and Class Members actual, statutory, punitive, and/or any other form of damages provided by and pursuant to the statutes cited above;

c. For an order awarding Plaintiffs and Class Members restitution, disgorgement and/or other equitable relief provided by and pursuant to the statutes cited above or as the Court deems proper;

d. For an order or orders requiring Defendant to adequately remediate the Breach and its effects.

e. For an order awarding Plaintiffs and Class Members pre-judgment and post-judgment interest;

f. For an order awarding Plaintiffs and Class Members treble damages, other enhanced damages and attorneys' fees as provided for under the statutes cited above and related statutes;

g. For an order awarding Plaintiffs and the Class Members reasonable attorneys' fees and costs of suit, including expert witness fees;

h. For an order awarding such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

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

Dated: December 1, 2023

By: *Kyle McLean*

Kyle McLean (SBN 330580)
kmclean@sirillp.com
Mason Barney (*pro hac vice*)
mbarney@sirillp.com
Tyler Bean (*pro hac vice*)
tbean@sirillp.com
SIRI & GLIMSTAD LLP
700 S. Flower Street, Suite 1000
Los Angeles, CA 90017
Tel: (213) 376-3739

Nicholas A. Migliaccio (*pro hac vice* anticipated)
nmigliaccio@classlawdc.com
Jason S. Rathod (*pro hac vice* anticipated)
jrathod@classlawdc.com
MIGLIACCIO & RATHOD LLP
412 H Street NE, Suite 302
Washington, DC, 20002
Tel: (202) 470-3520

Kristen Lake Cardoso (SBN 338762)
cardoso@kolawyers.com
Jeff Ostrow (*pro hac vice* anticipated)
ostrow@kolawyers.com
Kenneth Grunfeld (*pro hac vice* anticipated)
grunfeld@kolawyers.com
KOPELOWITIZ OSTROW P.A.
One West Las Olas Blvd., Suite 500
Fort Lauderdale, FL 33301
Tel: (954) 525-4100

Interim Class Counsel for the Plaintiffs and Proposed Class

John J. Nelson (SBN 317598)
jnelson@milberg.com
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
280 S. Beverly Drive
Beverly Hills, CA 90212
Tel: (858) 209-6941

Eric Lechtzin (SBN 248958)
elechtzin@edelson-law.com
EDELSON LECHTZIN LLP
411 S. State Street, Suite N-300
Newtown, PA 18940
Tel: (215) 867-2399

Additional Counsel for the Plaintiffs and Proposed Class