

1 Kyle McLean (SBN #330580)

2 Email: kmclean@sirillp.com

3 Mason Barney*

4 Email: mbarney@sirillp.com

5 Tyler Bean*

6 Email: tbean@sirillp.com

7 **SIRI & GLIMSTAD LLP**

8 700 S. Flower Street, Ste. 1000

9 Los Angeles, CA 90017

10 Telephone: 213-376-3739

11 *Attorneys for Plaintiff and the Class*

12 **UNITED STATES DISTRICT COURT**
13 **CENTRAL DISTRICT OF CALIFORNIA**
14 **SOUTHERN DIVISION**

15 MANDI PETERSON, on behalf of
16 herself and all others similarly situated,

17 Plaintiff,

18 v.

19 VIVENDI TICKETING US LLC d/b/a
20 SEE TICKETS,

21 Defendant.

Case No.

CLASS ACTION COMPLAINT

Jury Trial Demanded

22 Plaintiff Mandi Peterson, individually and on behalf of the Class defined below of
23 similarly situated persons (“Plaintiff”), alleges the following against Vivendi Ticketing
24 US LLC d/b/a See Tickets (“Vivendi” or “Defendant”) based upon personal knowledge
25 with respect to herself and on information and belief derived from, among other things,
26 investigation of counsel and review of public documents as to all other matters. This
27 Court has jurisdiction over the Defendant because Defendant operates and has its
28 principal place of business in this District, and the computer systems implicated in this
Data Breach are likely based in and/or controlled in this District.

1 **INTRODUCTION**

2 1. Plaintiff brings this class action against Defendant for its failure to properly
3 secure and safeguard Plaintiff’s and other similarly situated customers’ payment card
4 information and other sensitive records as part of a computer hack that Defendant’s lax
5 permitted to occur.

6 2. Vivendi Ticketing US LLC d/b/a See Tickets is one of the leaders in the
7 global ticketing market, with a strong presence in Europe and the United States for events
8 such as concerts, shows, festivals, museums, theaters, trade fairs, exhibitions, and
9 sporting events.

10 3. Vivendi Ticketing US LLC d/b/a See Tickets is a wholly owned subsidiary
11 of Vivendi Village, which is the live entertainment and ticketing business unit of Vivendi
12 SE, the Vivendi media and communications group.

13 4. Defendant provided ticketing services to events where Plaintiff purchased
14 event tickets and, in making those purchases, turned her sensitive financial and other
15 personal information over to Defendant for what she believed would be safekeeping.

16 5. However, in May of 2023, Defendant was alerted to unusual activity on
17 certain of its e-commerce websites. Specifically, Defendant asserts that unauthorized
18 parties inserted multiple instances of malicious code into a number of its e-commerce
19 checkout pages, resulting in unauthorized access to, and acquisition of, certain customer
20 payment card information, including that belonging to Plaintiff.

21 6. Affected information includes customer names, addresses, and payment
22 card information (the “Private Information”) provided by customers (including Plaintiff)
23 through purchases made on the See Tickets website¹ between February 28, 2023 and July
24 2, 2023 (the “Data Breach”).

25
26
27 ¹ <https://www.seetickets.com>; with a specific url directed at customer in the United States,
28 <https://www.seetickets.us>.

1 7. On or about September 6, 2023, Defendant filed a data breach notice with
2 the Maine Attorney General’s office, reporting that over 323,498 customers were
3 affected.²

4 8. On or about that same day, Defendant began notifying affected individuals,
5 including Plaintiff. As of the date of this filing, there is no mention of the data breach on
6 Defendant’s website. This means that Plaintiff and Class Members had no idea their
7 private information had been compromised for at least five (5) months after Defendant
8 knew or should have known, and that they were, and continue to be, at significant risk of
9 identity theft and various other forms of personal, social, and financial harm. The risk
10 will remain for their respective lifetimes.

11 9. Defendant’s Notice of Data Breach Letters (the “**Notice Letter**”) disclosed
12 information regarding the data breach. Based on just the details in those letters it appears
13 that the information compromised in the Data Breach included highly sensitive data that
14 represents a gold mine for data thieves, such as customer name, address, zip code,
15 payment card number, expiration date, CVV number, (collectively the “Private
16 Information”) and on information and belief potentially additional personally identifiable
17 information (“PII”) that Defendant collected and maintained.

18 10. Armed with the Private Information accessed in the Data Breach, and an
19 eighteen-month head start, data thieves can commit a variety of crimes including, e.g.,
20 making fraudulent purchases and committing identity theft such as opening new financial
21 accounts in Class Members’ names.

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

26 _____
27 ² See [https://apps.web.maine.gov/online/aeviewer/ME/40/9507cec8-0c8c-46b7-bccf-](https://apps.web.maine.gov/online/aeviewer/ME/40/9507cec8-0c8c-46b7-bccf-c8baea5b2477.shtml)
28 [c8baea5b2477.shtml](https://apps.web.maine.gov/online/aeviewer/ME/40/9507cec8-0c8c-46b7-bccf-c8baea5b2477.shtml) (last visited September 10, 2023).

1 12. Defendant also only offered one year of credit monitoring services, therefore
2 Plaintiff and Class Members will also be forced to incur out of pocket costs for, *e.g.*,
3 purchasing credit monitoring services, credit freezes, credit reports, or other protective
4 measures to deter and detect identity theft.

5 13. Plaintiff has also already experienced fraudulent misuse of her payment card
6 information.

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

13 15. Importantly, this is the second major data breach that SeeTickets has
14 reported in less than a year's time. In October of 2022, Defendant reported a different
15 data breach that impacted over 400,000 customers' payment card data.³

16 16. Plaintiff brings this class action lawsuit to address Defendant's inadequate
17 safeguarding of Class Members' Private Information that it collected and maintained, and
18 for failing to provide timely and adequate notice to Plaintiff and Class Members that their
19 information had been subject to the unauthorized access and acquisition.

20 17. The potential for improper disclosure of Plaintiff's and Class Members'
21 Private Information was a known risk to Defendant, especially in light of the previously
22 reported data breach, and thus Defendant was on notice that failing to take steps necessary
23 to secure the Private Information from those risks left that property in a dangerous
24 condition.

25
26
27 ³ See [https://apps.web.maine.gov/online/aeviewer/ME/40/86fc7ff5-d406-422d-889c-](https://apps.web.maine.gov/online/aeviewer/ME/40/86fc7ff5-d406-422d-889c-d4e6abd62177.shtml)
28 [d4e6abd62177.shtml](https://apps.web.maine.gov/online/aeviewer/ME/40/86fc7ff5-d406-422d-889c-d4e6abd62177.shtml) (last visited on September 10, 2023).

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

4 19. Plaintiff's and Class Members' identities are now at risk because of
5 Defendant's negligent conduct, especially in light of the fraudulent misuse that has
6 already occurred.

7 20. Plaintiff seeks to remedy these harms on behalf of herself and all similarly
8 situated individuals whose Private Information was accessed and/or compromised during
9 the Data Breach.

10 21. Plaintiff seeks remedies including, but not limited to, compensatory
11 damages, reimbursement of out-of-pocket costs, and injunctive relief including long-term
12 improvements to Defendant's data security systems, future annual audits, and adequate
13 credit monitoring services funded by Defendant.

14 **PARTIES**

15 22. Plaintiff Mandi Peterson is, and at all times mentioned herein was, an
16 individual citizen of the State of Michigan.

17 23. Defendant Vivendi Ticketing US LLC d/b/a See Tickets is, and all times
18 mentioned herein was, a live entertainment and ticketing business incorporated in the
19 state of Delaware with its principal place of business at 6380 Wilshire Boulevard, Suite
20 900, Los Angeles, California 90048.

21 **JURISDICTION AND VENUE**

22 24. The Court has subject matter jurisdiction over this action under the Class
23 Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds \$5
24 million, exclusive of interest and costs. Upon information and belief, the number of class
25 members is over 100, many of whom have different citizenship from Defendant. Thus,
26 minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

1 25. This Court has jurisdiction over the Defendant because it operates and has
2 its principal place of business in this District, and the computer systems implicated in this
3 Data Breach are likely based in and/or controlled in this District.

4 26. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a
5 substantial part of the events giving rise to this action occurred in this District.

6 **DEFENDANT COLLECTS HIGHLY SENSITIVE CUSTOMER**
7 **INFORMATION**

8 27. Defendant is one of the leaders in the global ticketing market, with a strong
9 presence in Europe and the United States, and is a wholly owned subsidiary of Vivendi
10 Village, which is the live entertainment and ticketing business unit of Vivendi SE, the
11 Vivendi media and communications group.

12 28. Vivendi SE is a French mass media holding company that owns Gameloft,
13 Groupe Canal+, Havas, Editis, Prisma Media, Dailymotion, and Vivendi Village. Vivendi
14 SE reported its revenues in the first quarter of 2022 as \$2.76 billion.⁴

15 29. For the first quarter of 2022, Vivendi Village's revenues were \$31 million
16 as compared to \$8 million from the first quarter of 2021, a growth that is attributed to
17 dynamic ticketing activities under the See Tickets brand.⁵

18 30. Defendant provides ticketing services to producers and event organizers for
19 events such as concerts, shows, festivals, museums, theaters, trade fairs, exhibitions, and
20 sporting events.

21 31. When purchasing an event ticket on the See Tickets website, customers
22 provide:

- 23 • Email address
24 • Name;

25 _____
26 ⁴ 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.

27 ⁵ See Annual Report – Universal Registration Document 2021, Vivendi, available at
28 https://www.vivendi.com/wp-content/uploads/2022/04/20220404_VIV_Rapport-annuel-2021_VA.pdf
(last visited September 10, 2023).

- 1 • Address;
- 2 • Zip Code;
- 3 • Payment card information;
- 4 • Payment card expiration date; and
- 5 • CVV number.

6 32. At the time of the Data Breach, Defendant promised its customers that it
7 would not share this sensitive information with non-Vivendi owned companies third
8 parties.⁶ Other than sharing with financial organizations to process orders, and with
9 social media companies for marketing, the See Tickets privacy policy states:

10 See Tickets will only process your data with 3rd party
11 organizations if you have consented to hearing news and data
12 from them. See Tickets will specify who the data will be shared
13 with during the process of purchasing a ticket. The 3rd parties
14 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.

15 All 3rd party organizations must adhere to the General Data
16 Protection Act 2018.

17 33. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and
18 Class Members' Private Information, Defendant assumed legal and equitable duties and
19 knew or should have known, based, *inter alia*, on the nature of the information collected,
20 that it was responsible for protecting Plaintiff's and Class Members' Private Information
21 from disclosure.

22 34. Plaintiff and Class Members have taken reasonable steps to maintain the
23 confidentiality of their Private Information.

24 35. Plaintiff and Class Members relied on Defendant to keep their Private
25 Information confidential and securely maintained, to use this information for business
26 purposes only, and to make only authorized disclosures of this information.

27 ⁶ See *US Privacy Policy*, See Tickets, available at [https://misc.seetickets.us/privacy/](https://misc.seetickets.us/privacy/#informationwemaycollect)
28 [#informationwemaycollect](https://misc.seetickets.us/privacy/#informationwemaycollect) (last visited September 10, 2023).

DEFENDANT’S DATA BREACH AND NOTICE TO PLAINTIFF

1
2 36. Plaintiff and Class Members were Defendant’s customers. When customers
3 of Defendant make a purchase on the website, Defendant collects personal and financial
4 information, such as payment card information, along with name, address, and zip code.

5 37. Based on the Notice Letter filed by Defendant and sent to Plaintiff and Class
6 Members, it was alerted to activity indicating unauthorized access by a third party to
7 event checkout pages on the See Tickets website in May of 2023.

8 38. Defendant then learned that an unknown third party had obtained
9 unauthorized access to Defendant’s data starting in February of 2023. Defendant was
10 only able to stop the unauthorized access in July of 2023, two (2) months after initially
11 learning of the Data Breach and five (5) months after the Data Breach started.

12 39. In or around early September 2023, Defendant issued Notice Letters to
13 Plaintiff and Class Members, alerting them that their highly sensitive Private Information
14 had been exposed in a data breach. This means that Plaintiff and Class Members had no
15 idea their Private Information had been compromised for seven (7) months after
16 Defendant first learned about the Data Breach.

17 40. The Notice Letter then attached information about identity protection, and
18 listed generic steps that victims of data security incidents can take, such as examining
19 account statements, getting a copy of a free annual credit report, or implementing a fraud
20 alert or security freeze.

21 41. On information and belief, Defendant sent a similar generic letter to all
22 individuals affected.

23 42. Defendant had obligations created by contract, industry standards, common
24 law, and representations made to Plaintiff and Class Members to keep their Private
25 Information confidential and to protect it from unauthorized access and disclosure.

26 43. Plaintiff and Class Members provided their Private Information to
27 Defendant with the reasonable expectation and mutual understanding that Defendant
28

1 would comply with its obligations to keep such information confidential and secure from
2 unauthorized access and to provide timely notice of security breaches.

3 **DEFENDANT FAILED TO COMPLY WITH FTC GUIDELINES**

4 44. The Federal Trade Commission (“FTC”) has promulgated numerous guides
5 for businesses which highlight the importance of implementing reasonable data security
6 practices. According to the FTC, the need for data security should be factored into all
7 business decision making.

8 45. In October 2016, the FTC updated its publication, Protecting Personal
9 Information: A Guide for Business, which established cyber-security guidelines for
10 businesses. The guidelines note that businesses should protect the personal customer
11 information that they keep; properly dispose of personal information that is no longer
12 needed; encrypt information stored on computer networks; understand their network’s
13 vulnerabilities; and implement policies to correct any security problems. The guidelines
14 also recommend that businesses use an intrusion detection system to expose a breach as
15 soon as it occurs; monitor all incoming traffic for activity indicating someone is
16 attempting to hack the system; watch for large amounts of data being transmitted from
17 the system; and have a response plan ready in the event of a breach.

18 46. The FTC further recommends that companies not maintain PII longer than
19 is needed for authorization of a transaction; limit access to sensitive data; require complex
20 passwords to be used on networks; use industry-tested methods for security; monitor for
21 suspicious activity on the network; and verify that third-party service providers have
22 implemented reasonable security measures.

23 47. The FTC has brought enforcement actions against businesses for failing to
24 protect customer data adequately and reasonably, treating the failure to employ
25 reasonable and appropriate measures to protect against unauthorized access to
26 confidential consumer data as an unfair act or practice prohibited by Section 5 of the
27 Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. Orders resulting from these
28

1 actions further clarify the measures businesses must take to meet their data security
2 obligations.

3 48. On information and belief, Defendant failed to properly implement basic
4 data security practices. Defendant's failure to employ reasonable and appropriate
5 measures to protect against unauthorized access to patient PII constitutes an unfair act or
6 practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

7 49. Defendant was at all times fully aware of its obligation to protect the PII of
8 its customers.

9 **DEFENDANT FAILED TO COMPLY WITH INDUSTRY STANDARDS**

10 50. Experts studying cyber security routinely identify ecommerce platforms as
11 being particularly vulnerable to cyberattacks because of the value of the PII which they
12 collect and maintain.

13 51. Several best practices have been identified that a minimum should be
14 implemented by ecommerce providers like Defendant, including but not limited to
15 educating all employees; strong passwords; multi-layer security, including firewalls, anti-
16 virus, and anti-malware software; encryption, making data unreadable without a key;
17 multi-factor authentication; backup data, and; limiting which employees can access
18 sensitive data.

19 52. A number of industry and national best practices have been published and
20 should be used as a go-to resource when developing a business' cybersecurity standards.
21 The Center for Internet Security ("CIS") released its Critical Security Controls. The CIS
22 Benchmarks are the only consensus-based, best-practice security configuration guides
23 both developed and accepted by government, business, industry, and academia.⁷

24 53. Other best cybersecurity practices that are standard in the ecommerce
25 industry include installing appropriate malware detection software; monitoring and

26 _____
27 ⁷ *CIS Benchmarks FAQ*, Center for Internet Security, available at <https://www.cisecurity.org/cis-benchmarks/cis-benchmarks-faq> (last visited August 10, 2022).

1 limiting the network ports; protecting web browsers and email management systems;
2 setting up network systems such as firewalls, switches and routers; monitoring and
3 protection of physical security systems; protection against any possible communication
4 system; training staff regarding critical points.

5 54. Defendant failed to meet the minimum standards of any of the following
6 frameworks: the NIST Cybersecurity Framework Version 1.1 (including without
7 limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1,
8 PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and
9 RS.CO-2), and the Center for Internet Security’s Critical Security Controls (CIS CSC),
10 which are all established standards in reasonable cybersecurity readiness.

11 **FBI, FTC, NIST GUIDELINES ON PROTECTING CUSTOMER PERSONAL**
12 **INFORMATION**

13 55. Recently, the FBI issued a warning to companies about this exact type of
14 fraud. In the FBI’s Oregon FBI Tech Tuesday: Building a Digital Defense Against E-
15 Skimming, dated October 22, 2019, the agency stated:

16 This warning is specifically targeted to . . . businesses . . . that
17 take credit card payments online. E-skimming occurs when
18 cyber criminals inject malicious code onto a website. The bad
19 actor may have gained access via a phishing attack targeting
20 your employees—or through a vulnerable third-party vendor
attached to your company’s server.⁸

21 56. The FBI gave some stern advice to companies like Defendant:

22 Here’s what businesses and agencies can do to protect
23 themselves:

- 24 • Update and patch all systems with the latest security
software.
- 25 • Anti-virus and anti-malware need to be up-to-date and
firewalls strong.
- 26 • Change default login credentials on all systems.

27 ⁸ [https://www.fbi.gov/contact-us/field-offices/portland/news/press-releases/oregon-fbi-tech-tuesday-
28 building-a-digital-defense-agaist-e-skimming](https://www.fbi.gov/contact-us/field-offices/portland/news/press-releases/oregon-fbi-tech-tuesday-building-a-digital-defense-agaist-e-skimming)

- Educate employees about safe cyber practices. Most importantly, do not click on links or unexpected attachments in messages.
- Segregate and segment network systems to limit how easily cyber criminals can move from one to another.

57. But Defendant apparently did not take this advice because hackers scraped customers' Private Information off its website for a period of at least five (5) months until Defendant was able to cease the unauthorized access in July of 2023.

58. Similarly, the Federal Trade Commission ("FTC") has held that the failure to employ reasonable measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the FTC Act (codified by 15 U.S.C. § 45).

59. Under the FTC Act, Defendant are 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.

60. Beginning in 2007, the FTC released a set of industry standards related to data security and the data security practices of businesses, called "Protecting Personal Information: A Guide for Businesses" (the "FTC Guide"). In 2011, this guidance was updated to include fundamental data security principles for businesses. In addition to the necessity to protect consumer data, the guide established that:

- Businesses should dispose of personal identifiable information that is no longer needed;
- Businesses should encrypt personal identifiable information and protected cardholder data stored on computer networks so that it is unreadable even if hackers are able to gain access to the information;
- Businesses should thoroughly understand the types of vulnerabilities on their network (of which malware on a point-of-sale system is one) and how to address said vulnerabilities;

- Businesses should implement protocols necessary to correct security breaches;
- Businesses should install intrusion detection systems to expose security breaches at the moment they occur;
- Businesses should install monitoring mechanisms to watch for massive troves of data being transmitted from their systems; and,
- Businesses should have an emergency plan prepared in response to a breach.

61. On information and belief, Defendant failed to adequately address the foregoing requirements in the FTC Guide.

62. In 2015, the FTC supplemented the FTC Guide with a publication called “Start with Security” (the “Supplemented FTC Guide”). This supplement added further requirements for businesses that maintain customer data on their networks:

- Businesses should not keep personal identifiable information and protected cardholder data stored on their networks for any period longer than what is needed for authorization;
- Businesses should use industry-tested methods for data security; and,
- Businesses should be continuously monitoring for suspicious activity on their network.

63. Again, Defendant apparently failed to adequately address these requirements enumerated in the Supplemented FTC Guide.

64. The FTC Guide is clear that businesses should, among other things: (1) protect the personal customer information they acquire; (2) properly dispose of personal information that is no longer needed; (3) encrypt information stored on computer networks; (4) understand their network’s vulnerabilities; and (5) implement policies for installing vendor-approved patches to correct security vulnerabilities. The FTC guidance also recommends that businesses: (1) use an intrusion detection system to expose a breach as soon as it occurs; (2) monitor all incoming traffic for activity indicating that someone

1 may be trying to penetrate the system; and (3) watch for large amounts of data being
2 transmitted from the system. Plaintiff believes that Defendant did not follow these
3 recommendations, and as a result exposed hundreds of thousands of consumers to harm.

4 65. Furthermore, the FTC has issued orders against businesses for failing to
5 employ reasonable measures to safeguard customer data. The orders provide further
6 public guidance to businesses concerning their data security obligations.

7 66. Defendant knew or should have known about their obligation to comply with
8 the FTC Act, the FTC Guide, the Supplemented FTC Guide, and many other FTC
9 pronouncements regarding data security.

10 67. Thus, among other things, Defendant's misconduct violated the FTC Act
11 and the FTC's data security pronouncements, which led to the Data Breach, and resulted
12 directly and proximately in harm to Plaintiff and Class Members.

13 68. Additionally, the National Institute of Standards and Technology (NIST)
14 provides basic network security guidance that enumerates steps to take to avoid
15 cybersecurity vulnerabilities. Although use of NIST guidance is voluntary, the guidelines
16 provide valuable insights and best practices to protect network systems and data.

17 69. NIST guidance includes recommendations for risk assessments, risk
18 management strategies, system access controls, training, data security, network
19 monitoring, breach detection, and mitigation of existing anomalies.

20 70. Defendant's failure to protect massive amounts of Payment Information
21 throughout the multi-month breach period belies any assertion that Defendant employed
22 proper data security protocols or adhered to the spirit of the NIST guidance.

23 **DEFENDANT'S SECURITY OBLIGATIONS**

24 71. Defendant breached its obligations to Plaintiff and Class Members and/or
25 was otherwise negligent and reckless because they failed to properly maintain and
26 safeguard their computer systems and data. Defendant's unlawful conduct includes, but
27 is not limited to, the following acts and/or omissions:
28

- 1 a. Failing to maintain an adequate data security system to reduce the risk of
- 2 data breaches and cyber-attacks;
- 3 b. Failing to adequately protect customers' Private Information;
- 4 c. Failing to properly monitor its own data security systems for existing
- 5 intrusions;
- 6 d. Failing to fully comply with FTC guidelines for cybersecurity, in violation
- 7 of Section 5 of the FTC Act, and;
- 8 e. Failing to adhere to industry standards for cybersecurity.

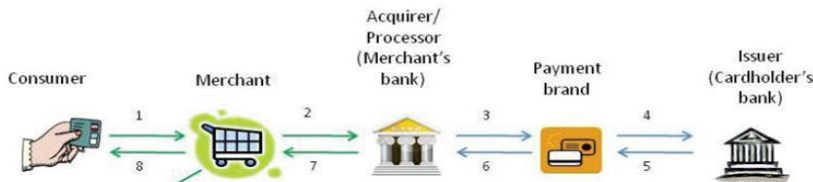
9 72. On information and belief, as the result of computer systems in need of
10 security upgrading, inadequate procedures for handling emails containing viruses or other
11 malignant computer code, and employees who opened files containing the virus or
12 malignant code that perpetrated the cyberattack, Defendant negligently and unlawfully
13 failed to safeguard Plaintiff's and Class Members' Private Information.

14 73. Accordingly, as outlined below, Plaintiff's and Class Members' daily lives
15 were severely disrupted. What's more, Plaintiff has already experienced (and Plaintiff
16 and Class Members now face an increased risk of) fraud and identity theft as a direct
17 result of the Data Breach. Plaintiff and Class Members also lost the benefit of the bargain
18 they made with Defendant as its customers.

19 **DATA BREACHES, FRAUD AND IDENTITY THEFT**

20 74. In a debit or credit card purchase transaction, card data must flow through
21 multiple systems and parties to be processed. Generally, the cardholder presents a credit
22 or debit card to an e-commerce retailer (through an e-commerce website) to pay for
23 merchandise. The card is then "swiped" and information about the card and the purchase
24 is stored in the retailer's computers and then transmitted to the acquirer or processor (i.e.,
25 the retailer's bank). The acquirer relays the transaction information to the payment card
26 company, who then sends the information to the issuer (i.e., cardholder's bank). The
27
28

1 issuer then notifies the payment card company of its decision to authorize or reject the
 2 transaction. See graphic below:⁹



1	The consumer selects a card for payment. The cardholder data is entered into the merchant's payment system, which could be the point-of-sale (POS) terminal/software or an e-commerce website.
2	The card data is sent to an acquirer/payment processor, whose job it is to route the data through the payments system for processing. With e-commerce transactions, a "gateway" provider may provide the link from the merchant's website to the acquirer.
3	The acquirer/processor sends the data to the payment brand (e.g. Visa, MasterCard, American Express, etc.) who forward it to the issuing bank/issuing bank processor
4	The issuing bank/processor verifies that the card is legitimate, not reported lost or stolen, and that the account has the appropriate amount of credit/funds available to pay for the transaction.
5	If so, the issuer generates an authorization number and routes this number back to the card brand. With the authorization, the issuing bank agrees to fund the purchase on the consumer's behalf.
6	The card brand forwards the authorization code back to the acquirer/processor.
7	The acquirer/processor sends the authorization code back to the merchant.
8	The merchant concludes the sale with the customer.

13 75. There are two points in the payment process where sensitive cardholder data
 14 is at risk of being exposed or stolen: pre-authorization when the merchant has captured a
 15 consumer's data and it is waiting to be sent to the acquirer; and post-authorization when
 16 cardholder data has been sent back to the merchant with the authorization response from
 17 the acquirer, and it is placed into some form of storage in the merchant's servers.

18 76. Encryption mitigates security weaknesses that exist when cardholder data
 19 has been stored, but not yet authorized, by using algorithmic schemes to transform plain
 20 text information into a non-readable format called "ciphertext." By scrambling the
 21 payment card data the moment it is "swiped," hackers who steal the data are left with
 22 useless, unreadable text in the place of payment card numbers accompanying the
 23 cardholder's personal information stored in the retailer's computers.

24
 25 ⁹"Payments 101: Credit and Debit Card Payments," (First Data) available at
 26 <http://euro.ecom.cmu.edu/resources/elibrary/epay/Payments-101.pdf> (last visited October 27, 2022);
 27 see also "Payments 101: An Intro to Card Networks and Card Transactions" (Very Good Security),
 28 available at <https://www.verygoodsecurity.com/blog/posts/payments-101-an-intro-to-card-networks-and-card-transactions> (last visited October 27, 2022).

1 77. However, when the data is not encrypted, hackers can target what they refer
2 to as the *fullz*—a term used by criminals to refer to stealing the full primary account
3 number, card holder contact information, credit card number, CVC code, and expiration
4 date. The *fullz* is exactly what appears to have been scraped from Defendant’s ecommerce
5 platform. Typically, these hackers insert virtual credit card skimmers or scrapers (also
6 known as *formjacking*) into a web application (usually the shopping cart) and proceed to
7 scrape credit card information to sell on the dark web.¹⁰

8 78. At the very least, Defendant chose not to invest in the technology to encrypt
9 payment card data at point-of-sale to make its customers’ data more secure, despite
10 already having just experienced a similar data breach only months before, and failed to
11 install updates, patches, and malware protection or to install them in a timely manner to
12 protect against a data security breach, and/or failed to provide sufficient control employee
13 credentials and access to computer systems to prevent a security breach and/or theft of
14 payment card data.

15 79. The FTC hosted a workshop to discuss “informational injuries” which are
16 injuries that consumers suffer from privacy and security incidents, such as data breaches
17 or unauthorized disclosure of data.¹¹ Exposure of personal information that a consumer
18 wishes to keep private may cause both market and non-market harm to the consumer,
19 such as the ability to obtain or keep employment and negative impact on consumer’s
20 relationships with family, friends, and coworkers. Consumers’ loss of trust in e-
21 commerce also deprives them of the benefits provided by the full range of goods and
22 services available which can have negative impacts on daily life.

23
24
25 ¹⁰ *Magecart Hits 80 Major eCommerce Sites in Card-Skimming Bonanza*, Threatpost (August 28,
2019), available at: <https://threatpost.com/magecart-ecommerce-card-skimming-bonanza/147765/>.

26 ¹¹ *FTC Information Injury Workshop, BE and BCP Staff Perspective*, Federal Trade Commission,
27 (October 2018), available at [https://www.ftc.gov/system/files/documents/reports/ftc-informational-
28 _injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-
_oct_2018_0.pdf](https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf).

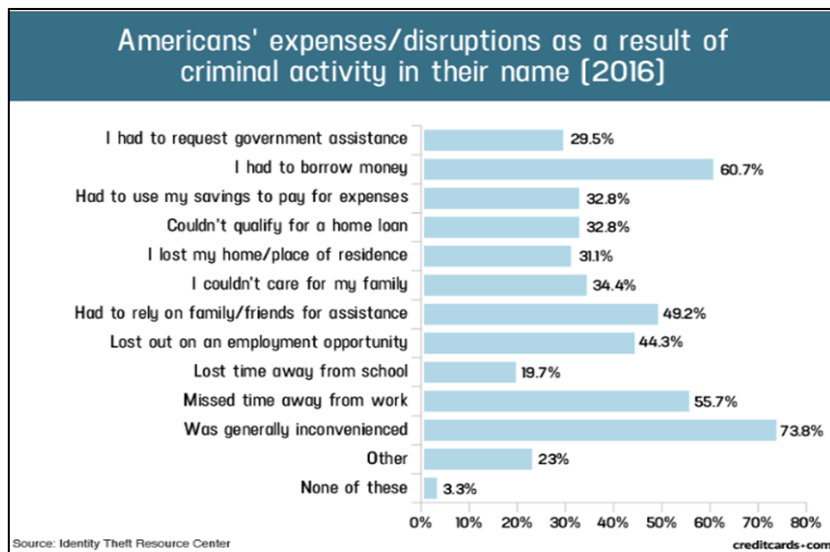
1 80. Any victim of a data breach is exposed to serious ramifications regardless
2 of the nature of the data. Indeed, the reason criminals steal information is to monetize it.
3 They do this by selling the spoils of their cyberattacks on the black market to identity
4 thieves who desire to extort and harass victims or take over victims' identities in order to
5 engage in illegal financial transactions under the victims' names. Because a person's
6 identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about
7 a person, the easier it is for the thief to take on the victim's identity, or otherwise harass
8 or track the victim. For example, armed with just a name and date of birth, a data thief
9 can utilize a hacking technique referred to as "social engineering" to obtain even more
10 information about a victim's identity, such as a person's login credentials or Social
11 Security number. Social engineering is a form of hacking whereby a data thief uses
12 previously acquired information to manipulate individuals into disclosing additional
13 confidential or personal information through means such as spam phone calls and text
14 messages or phishing emails.

15 81. The detailed information potentially obtained in the instant data breach
16 regarding the nature of the purchases Plaintiff and Class Members made on the See
17 Tickets website makes the risk of phishing attacks even greater. With detailed purchase
18 information, criminals will be able to reference those specific purchases that Plaintiff and
19 Class Members will recognize, making it harder for Plaintiff and Class Members to
20 identify such phishing attacks.

21 82. The FTC recommends that identity theft victims take several steps to protect
22 their personal and financial information after a data breach, including contacting one of
23 the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7
24 years if someone steals their identity), reviewing their credit reports, contacting
25 companies to remove fraudulent charges from their accounts, placing a credit freeze on
26 their credit, and correcting their credit reports.¹²

27 _____
28 ¹² See *IdentityTheft.gov*, Federal Trade Commission, available at <https://www.identitytheft.gov/Steps>

1 83. A study by Identity Theft Resource Center shows the multitude of harms
2 caused by fraudulent use of PII:¹³



26 84. Moreover, theft of Private Information is also gravely serious. Its value is
27 axiomatic, considering the value of “big data” in corporate America and the fact that the
28 consequences of cyber thefts include heavy prison sentences. Even this obvious risk to
reward analysis illustrates beyond doubt that Private Information has considerable market
value.

85. It must also be noted there may be a substantial time lag – measured in years
-- between when harm occurs and when it is discovered, and between when Private
Information and/or financial information is stolen and when it is used. According to the
U.S. Government Accountability Office, which conducted a study regarding data
breaches:¹⁴

[L]aw enforcement officials told us that in some cases, stolen
data may be held for up to a year or more before being used to
commit identity theft. Further, once stolen data have been sold

(last visited August 11, 2022).

¹³ Steele, Jason, *Credit Card and ID Theft Statistics*, CreditCards.com (October 23, 2017), available at <https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276/>.

¹⁴ *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (June 2007), available at <https://www.gao.gov/assets/270/262904.html>.

1 or posted on the Web, fraudulent use of that information may
2 continue for years. As a result, studies that attempt to measure
3 the harm resulting from data breaches cannot necessarily rule
4 out all future harm.

5 86. Private Information is such a valuable commodity to identity thieves that
6 once the information has been compromised, criminals often trade the information on the
7 “cyber black market” for years.

8 87. There is a strong probability that entire batches of stolen information have
9 been dumped on the black market and are yet to be dumped on the black market, meaning
10 Plaintiff and Class Members are at an increased risk of fraud and identity theft for many
11 years into the future. Thus, Plaintiff and Class Members must vigilantly monitor their
12 financial accounts for many years to come.

13 **PLAINTIFF’S AND CLASS MEMBERS’ DAMAGES**

14 88. Plaintiff and Class Members have been damaged by the compromise of their
15 Private Information in the Data Breach.

16 89. Plaintiff’s Private Information, including her sensitive payment card data,
17 was compromised as a direct and proximate result of the Data Breach and subsequently
18 misused. Specifically, the payment card Plaintiff used to make purchases on Defendant’s
19 website was recently used to make fraudulent purchases totaling roughly \$1,000.00. She
20 is still waiting for this money to be put back into her account once the dispute process is
21 settled, but there is no guarantee that she will get the full amount back.

22 90. As a direct and proximate result of Defendant’s conduct, Plaintiff and Class
23 Members have been placed at an imminent, immediate, and continuing increased risk of
24 harm from fraud and identity theft.

25 91. As a direct and proximate result of Defendant’s conduct, Plaintiff and Class
26 Members have been forced to spend time dealing with the effects of the Data Breach.

27 92. Plaintiff and Class Members face substantial risk of out-of-pocket fraud
28 losses such as fraudulent transactions similar to those already experienced by Plaintiff

1 Peterson, loans opened in their names, tax return fraud, utility bills opened in their names,
2 credit card fraud, and similar identity theft.

3 93. Plaintiff and Class Members face substantial risk of being targeted for future
4 phishing, data intrusion, and other illegal schemes based on their Private Information as
5 potential fraudsters could use that information to target such schemes more effectively to
6 Plaintiff and Class Members.

7 94. Plaintiff and Class Members may also incur out-of-pocket costs for
8 protective measures such as credit monitoring fees, credit report fees, credit freeze fees,
9 along with other similar costs directly or indirectly related to the Data Breach.

10 95. The information that Defendant maintains regarding Plaintiff and Class
11 Members, when combined with publicly available information, would allow nefarious
12 actors to paint a complete financial and personal history of Plaintiff and Class Members.

13 96. Plaintiff and Class Members were also damaged via benefit-of-the-bargain
14 damages. Plaintiff and Class Members overpaid for a service that was intended to be
15 accompanied by adequate data security but was not. Part of the price Plaintiff and Class
16 Members paid to Defendant was intended to be used by Defendant to fund adequate
17 security of Defendant's computer property and protect Plaintiff's and Class Members'
18 Private Information. Thus, Plaintiff and Class Members did not get what they paid for.

19 97. Plaintiff and Class Members have spent and will continue to spend
20 significant amounts of time monitoring their financial and medical accounts and records
21 for misuse.

22 98. Plaintiff and Class Members have suffered or will suffer actual injury as a
23 direct result of the Data Breach. Many victims suffered ascertainable losses in the form
24 of out-of-pocket expenses and the value of their time reasonably incurred to remedy or
25 mitigate the effects of the Data Breach relating to:

- 26 a. Finding fraudulent charges;
- 27 b. Canceling and reissuing credit and debit cards;

- 1 c. Purchasing credit monitoring and identity theft prevention;
- 2 d. Addressing their inability to withdraw funds linked to compromised
- 3 accounts;
- 4 e. Taking trips to banks and waiting in line to obtain funds held in
- 5 limited accounts;
- 6 f. Placing “freezes” and “alerts” with credit reporting agencies;
- 7 g. Spending time on the phone with or at a financial institution to dispute
- 8 fraudulent charges;
- 9 h. Contacting financial institutions and closing or modifying financial
- 10 accounts;
- 11 i. Resetting automatic billing and payment instructions from
- 12 compromised credit and debit cards to new ones;
- 13 j. Paying late fees and declined payment fees imposed as a result of
- 14 failed automatic payments that were tied to compromised cards that
- 15 had to be cancelled; and
- 16 k. Closely reviewing and monitoring bank accounts and credit reports
- 17 for unauthorized activity for years to come.

18 99. Moreover, Plaintiff and Class Members have an interest in ensuring that
19 their Private Information, which is believed to remain in the possession of Defendant, is
20 protected from further breaches by the implementation of security measures and
21 safeguards, including but not limited to, making sure that the storage of data or documents
22 containing personal and financial information is not accessible online, that access to such
23 data is password-protected, and that such data is properly encrypted.

24 100. As a direct and proximate result of Defendant’s actions and inactions,
25 Plaintiff and Class Members have suffered a loss of privacy and either have suffered harm
26 or are at an imminent and increased risk of future harm.

27 **CLASS ACTION ALLEGATIONS**

1 101. Plaintiff brings this action pursuant to Rule 23 of the Federal Rules of Civil
2 Procedure on behalf of herself and on behalf of all other persons similarly situated.

3 102. Plaintiff proposes the following Class definitions, subject to amendment as
4 appropriate:

5 **Nationwide Class** (the “Class”)

6 All individuals in the United States whose Private Information
7 was subject to the Data Breach announced by Defendant on or
8 about September 6, 2023, including those who Defendant
9 identified as being among those individuals impacted by the Data
Breach, and all persons who were sent a notice of the Data
Breach.

10 103. Excluded from the above Class are Defendant and their parents or
11 subsidiaries, any entities in which it has a controlling interest, as well as its officers,
12 directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns.
13 Also excluded are any Judge to whom this case is assigned as well as his or her judicial
14 staff and immediate family members.

15 104. Plaintiff reserves the right to modify or amend the definitions of the
16 proposed Class before the Court determines whether certification is appropriate.

17 105. The proposed Class meets the criteria for certification under Fed. R. Civ. P.
18 23(a), (b)(2), and (b)(3).

19 106. Numerosity. The Class Members are so numerous that joinder of all
20 members is impracticable. According to disclosures made to the Maine Attorney General,
21 323,498 individuals were affected. The identities of Class Members are ascertainable
22 through Defendant’s records, Class Members’ records, publication notice, self-
23 identification, and other means.

24 107. Commonality. There are questions of law and fact common to the Class,
25 which predominate over any questions affecting only individual Class Members. These
26 common questions of law and fact include, without limitation:

27 a. Whether Defendant engaged in the conduct alleged herein;
28

- 1 b. When Defendant actually learned of the data breach and whether its
- 2 response was adequate;
- 3 c. Whether Defendant unlawfully used, maintained, lost, or disclosed
- 4 Plaintiff's and Class Members' Private Information;
- 5 d. Whether Defendant failed to implement and maintain reasonable
- 6 security procedures and practices appropriate to the nature and scope
- 7 of the information compromised in the Data Breach;
- 8 e. Whether Defendant's data security systems prior to and during the
- 9 Data Breach complied with applicable data security laws and
- 10 regulations;
- 11 f. Whether Defendant's data security systems prior to and during the
- 12 Data Breach were consistent with industry standards;
- 13 g. Whether Defendant owed a duty to Class Members to safeguard their
- 14 Private Information;
- 15 h. Whether Defendant breached their duty to Class Members to
- 16 safeguard their Private Information;
- 17 i. Whether computer hackers obtained Class Members' Private
- 18 Information in the Data Breach;
- 19 j. Whether Defendant had a legal duty to provide timely and accurate
- 20 notice of the data breach to Plaintiff and Class Members;
- 21 k. Whether Defendant breached its duty to provide timely and accurate
- 22 notice of the data breach to Plaintiff and Class Members;
- 23 l. Whether Defendant knew or should have known that its data security
- 24 systems and monitoring processes were deficient;
- 25 m. What damages Plaintiff and Class Members suffered as a result of
- 26 Defendant's misconduct;
- 27 n. Whether Defendant's conduct was negligent;
- 28

- 1 o. Whether Defendant's conduct was *per se* negligent;
- 2 p. Whether Defendant was unjustly enriched;
- 3 q. Whether Plaintiff and Class Members are entitled to additional credit
- 4 or identity monitoring and are entitled to other monetary relief; and
- 5 r. Whether Plaintiff and Class Members are entitled to equitable relief,
- 6 including injunctive relief, restitution, disgorgement, and/or the
- 7 establishment of a constructive trust.

8 108. Typicality. Plaintiff's claims are typical of those of other Class Members
9 because Plaintiff's Private Information, like that of every other Class Member, was
10 compromised in the Data Breach.

11 109. Adequacy of Representation. Plaintiff will fairly and adequately represent
12 and protect the interests of the Members of the Class. Plaintiff's Counsel is competent
13 and experienced in litigating class actions, including data privacy litigation of this kind.

14 110. Predominance. Defendant has engaged in a common course of conduct
15 toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data
16 was stored on the same computer systems and unlawfully accessed in the same way. The
17 common issues arising from Defendant's conduct affecting Class Members set out above
18 predominate over any individualized issues. Adjudication of these common issues in a
19 single action has important and desirable advantages of judicial economy.

20 111. Superiority. A Class action is superior to other available methods for the fair
21 and efficient adjudication of the controversy. Class treatment of common questions of
22 law and fact is superior to multiple individual actions or piecemeal litigation. Absent a
23 Class action, most Class Members would likely find that the cost of litigating their
24 individual claims is prohibitively high and would therefore have no effective remedy.
25 The prosecution of separate actions by individual Class Members would create a risk of
26 inconsistent or varying adjudications with respect to individual Class Members, which
27 would establish incompatible standards of conduct for Defendant. In contrast, the conduct
28

1 of this action as a Class action presents far fewer management difficulties, conserves
2 judicial resources and the parties' resources, and protects the rights of each Class
3 member.

4 112. Class certification also is appropriate under Fed. R. Civ. P. 23(b)(2).
5 Defendant has acted or has refused to act on grounds generally applicable to the Class,
6 so that final injunctive relief or corresponding declaratory relief is appropriate as to the
7 Class as a whole.

8 113. Finally, all members of the proposed Class are readily ascertainable.
9 Defendant has access to Class Members' names and addresses affected by the Data
10 Breach. Class Members have already been preliminarily identified and sent notice of the
11 Data Breach by Defendant.

12 **CLAIMS FOR RELIEF**

13 **COUNT I**
14 **NEGLIGENCE**

15 **(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)**

16 114. Plaintiff restates and realleges the allegations in the preceding paragraphs as
17 if fully set forth herein.

18 115. Defendant knowingly collected, came into possession of, and maintained
19 Plaintiff's and Class Members' Private Information, and had a duty to exercise reasonable
20 care in safeguarding, securing, and protecting such information from being compromised,
21 lost, stolen, misused, and/or disclosed to unauthorized parties.

22 116. Defendant knew, or should have known, of the risks inherent in collecting
23 the Private Information of Plaintiff and Class Members and the importance of adequate
24 security, especially in light of its recent data security issues that have now resulted in two
25 major data breaches within the last two years.

1 117. Defendant owed a duty of care to Plaintiff and Class Members whose Private
2 Information was entrusted to them. Defendant's duties included, but were not limited to,
3 the following:

- 4 a. To exercise reasonable care in obtaining, retaining, securing,
5 safeguarding, deleting and protecting Private Information in their
6 possession;
- 7 b. To protect customers' Private Information using reasonable and adequate
8 security procedures and systems that are compliant with the industry
9 standards;
- 10 c. To have procedures in place to prevent the loss or unauthorized
11 dissemination of Private Information in their possession;
- 12 d. To employ reasonable security measures and otherwise protect the
13 Private Information of Plaintiff and Class Members pursuant to
14 California law (where Defendant is headquartered), specifically the
15 Customer Records Act, Cal. Civ. Code § 1798.80, *et seq.*;
- 16 e. To implement processes to quickly detect a data breach and to timely act
17 on warnings about data breaches; and
- 18 f. To promptly notify Plaintiff and Class Members of the Data Breach, and
19 to disclose precisely the type(s) of information compromise.

20 118. Plaintiff and Class Members were foreseeable and probable victims of any
21 inadequate security practices, and Defendant owed them a duty of care not to subject
22 them to an unreasonable risk of harm.

23 119. Defendant, through its actions and/or omissions, unlawfully breached its
24 duty to Plaintiff and Class members by failing to exercise reasonable care in protecting
25 and safeguarding Plaintiff's and Class Members' Private Information within Defendant's
26 possession.

1 120. Defendant, by its actions and/or omissions, breached its duty of care by
2 failing to provide, or by acting with reckless disregard for, fair, reasonable, or adequate
3 computer systems and data security practices to safeguard the Private Information of
4 Plaintiff and Class Members.

5 121. Defendant, by its actions and/or omissions, breached its duty of care by
6 failing to promptly identify the Data Breach and then provide prompt notice of the Data
7 Breach to the persons whose Private Information was compromised.

8 122. Defendant acted with reckless disregard for the rights of Plaintiff and Class
9 Members by failing to provide prompt and adequate individual notice of the Data Breach
10 so that they could take measures to protect themselves from damages caused by the
11 fraudulent use of the Private Information compromised in the Data Breach.

12 123. Defendant had a special relationship with Plaintiff and Class Members.
13 Plaintiff's and Class Members' willingness to entrust Defendant with their Private
14 Information was predicated on the understanding that Defendant would take adequate
15 data security precautions. Moreover, only Defendant had the ability to protect its systems
16 (and the Private Information that it stored thereon) from unauthorized access and
17 disclosure.

18 124. Defendant's breach of duties owed to Plaintiff and Class Members caused
19 Plaintiff's and Class Members' Private Information to be compromised.

20 125. Defendant's breaches of duty caused a foreseeable risk of harm to Plaintiff
21 and Class Members to suffer from identity theft, loss of time and money to monitor their
22 finances for fraud, and loss of control over their Private Information.

23 126. As a result of Defendant's negligence and breach of duties, Plaintiff and
24 Class Members are in danger of imminent harm in that their Private Information, which
25 is still in the possession of third parties, and which, in Plaintiff's case, has already been
26 misused for fraudulent purposes.

1 127. Defendant also had independent duties under state laws that required it to
2 reasonably safeguard Plaintiff’s and Class Members’ Private Information and promptly
3 notify them about the Data Breach.

4 128. But for Defendant’s wrongful and negligent breach of the duties it owed
5 Plaintiff and Class Members, their Private Information either would not have been
6 compromised or they would have been able to prevent some or all of the damages alleged
7 herein to have been suffered.

8 129. As a direct and proximate result of Defendant’s negligent conduct, Plaintiff
9 and Class Members have suffered damages and are at imminent risk of further harm.

10 130. The injury and harm that Plaintiff and Class Members suffered (as alleged
11 above) was reasonably foreseeable.

12 131. The injury and harm that Plaintiff and Class Members suffered (as alleged
13 above) was the direct and proximate result of Defendant’s negligent conduct.

14 132. Plaintiff and Class Members have suffered injury and are entitled to
15 damages in an amount to be proven at trial.

16 133. In addition to monetary relief and in light of Defendant’s recent data
17 breaches, Plaintiff and Class Members also are entitled to injunctive relief requiring
18 Defendant to, *inter alia*, strengthen its data security systems and monitoring procedures,
19 conduct periodic audits of those systems, and provide lifetime credit monitoring and
20 identity theft insurance to Plaintiff and Class Members.

21 **COUNT II**
22 **NEGLIGENCE *PER SE***
23 **(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)**

24 134. Plaintiff restates and realleges the allegations in the preceding paragraphs as
25 if fully set forth herein.

26 135. Pursuant to Section 5 of the Federal Trade Commission Act (“FTCA”), 15
27 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and
28

1 data security to safeguard the Private Information, including payment card information,
2 of Plaintiff and Class Members.

3 136. Plaintiff and Class Members are within the class of persons that the FTCA
4 is intended to protect.

5 137. The FTCA prohibits “unfair . . . practices in or affecting commerce,”
6 including, as interpreted and enforced by the FTC, the unfair act or practice of failing to
7 use reasonable measures to protect Private Information. The FTC publications described
8 above, and the industry standard data and cybersecurity measures, also form part of the
9 basis of Defendant’s duty in this regard.

10 138. Defendant violated the FTCA by failing to use reasonable data security
11 measures to protect the Private Information of Plaintiff and the Class and not complying
12 with applicable industry standards, as described herein.

13 139. Defendant’s violations of the FTCA constitute negligence *per se*.

14 140. In connection with its consumer transactions, Defendant engaged in unfair,
15 abusive or deceptive acts, omissions or practices by misrepresenting material facts to
16 Plaintiff and the Class and by representing that it did and would comply with the
17 requirements of relevant federal and state law pertaining to the privacy and security of
18 Plaintiff’s and Class Members’ Private Information. Such requirements included, but are
19 not limited to, those imposed by laws such as the FTCA.

20 141. It was reasonably foreseeable that the failure to reasonably protect and
21 secure Plaintiff’s and Class Members’ Private Information in compliance with applicable
22 laws would result in an unauthorized third-party gaining access to Defendant’s servers,
23 networks, databases, and/or computers that stored or contained Plaintiff’s and Class
24 Members’ Private Information.

25 142. Plaintiff’s and Class Members’ Private Information constitutes personal
26 property that was stolen due to Defendant’s negligence, resulting in harm, injury and
27 damages to Plaintiff and Class Members.

1 143. As a direct and proximate result of Defendant’s negligence *per se*, Plaintiff
2 and the Class have suffered, and continue to suffer, injuries and damages arising from the
3 unauthorized access of their Private Information, including payment card data, as a result
4 of the Data Breach, including but not limited to, damages from the actual misuse of their
5 Private Information and/or the lost time and effort to mitigate the actual and/or potential
6 impact of the Data Breach on their lives.

7 144. Defendant breached its duties to Plaintiff and the Class under these laws by
8 failing to provide fair, reasonable, or adequate computer systems and data security
9 practices to safeguard Plaintiff’s and Class Members’ Private Information.

10 145. But for Defendant’s wrongful and negligent breach of its duties owed to
11 Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

12 146. The injury and harm suffered by Plaintiff and Class Members was the
13 reasonably foreseeable result of Defendant’s breach of its duties. Defendant knew or
14 should have known that it was failing to meet its duties, and that another data breach
15 would cause Plaintiff and Class Members to experience the foreseeable harms associated
16 with the exposure of their Private Information.

17 147. As a direct and proximate result of Defendant’s negligence *per se*, Plaintiff
18 and Class Members have suffered, and continue to suffer, injuries damages arising from
19 their inability to use their debit or credit cards because those cards were cancelled,
20 suspended, or otherwise rendered unusable as a result of the data breach and/or false or
21 fraudulent charges stemming from the data breach, including but not limited to late fees
22 charges; damages from lost time and effort to mitigate the actual and potential impact of
23 the data breach on their lives including, *inter alia*, by contacting their financial
24 institutions to place to dispute fraudulent charges, closing or modifying financial
25 accounts, closely reviewing and monitoring their accounts for unauthorized activity.

1 148. As a direct and proximate result of Defendant’s negligent conduct, Plaintiff
2 and Class Members have suffered injury and are entitled to compensatory and
3 consequential damages in an amount to be proven at trial.

4 149. In addition to monetary relief and in light of Defendant’s recent data security
5 issues resulting in two major data breaches in the last two years, Plaintiff and Class
6 Members also are entitled to injunctive relief requiring Defendant to, *inter alia*,
7 strengthen its data security systems and monitoring procedures, conduct periodic audits
8 of those systems, and provide lifetime credit monitoring and identity theft insurance to
9 Plaintiff and Class Members.

10 **COUNT III**
11 **BREACH OF CONTRACT**
12 **(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)**

13 150. Plaintiff restates and realleges the allegations in the preceding paragraphs as
14 if fully set forth herein.

15 151. Plaintiff and Class Members entered into a valid and enforceable contract
16 when they paid money to Defendant in exchange for services, which included promises
17 to secure, safeguard, protect, keep private, and not disclose Plaintiff’s and Class
18 Members’ Private Information.

19 152. Defendant’s Privacy Policy memorialized the rights and obligations of
20 Defendant and its customers. This document was provided to Plaintiff in a manner and
21 during a time where it became part of the agreement for services.¹⁵

22 153. In the Privacy Policy, Defendant commits to protecting the privacy and
23 security of private information and promises to never share customer information aside
24 from limited exceptions.

25 154. Plaintiff and Class Members fully performed their obligations under their
26 contracts with Defendant.

27 _____
28 ¹⁵ Terms of Purchase *available at* <https://misc.seetickets.us/terms/>.

1 155. Defendant did not secure, safeguard, protect, and/or keep private Plaintiff's
2 and Class Members' Private Information and/or it disclosed their Private Information to
3 third parties, and therefore Defendant breached its contract with Plaintiff and Class
4 Members.

5 156. Defendant allowed third parties to access, copy, and/or transfer Plaintiff's
6 and Class Members' Private Information, without permission, and therefore Defendant
7 breached its contracts with Plaintiff and Class Members.

8 157. Defendant's failure to satisfy its confidentiality and privacy obligations
9 resulted in Defendant providing services to Plaintiff and Class Members that were of a
10 diminished value.

11 158. As a result, Plaintiff and Class Members have been harmed, damaged,
12 and/or injured as described herein.

13 159. In addition to monetary relief and in light of Defendant's recent data security
14 issues resulting in two major data breaches in the last two years, Plaintiff and Class
15 Members also are entitled to injunctive relief requiring Defendant to, *inter alia*,
16 strengthen its data security systems and monitoring procedures, conduct periodic audits
17 of those systems, and provide lifetime credit monitoring and identity theft insurance to
18 Plaintiff and Class Members.

19 **COUNT IV**
20 **BREACH OF IMPLIED CONTRACT**
21 **(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)**

22 160. Plaintiff restates and realleges the allegations in the preceding paragraphs as
23 if fully set forth herein.

24 161. Plaintiff brings this Count alternatively to Count III above.

25 162. Defendant provides ecommerce services to Plaintiff and Class Members.
26 Plaintiff and Class Members also formed an implied contract with Defendant regarding
27 the provision of those services through their collective conduct, including by Plaintiff and
28

1 Class Members paying for services and/or receiving goods in the form of event tickets
2 from Defendant.

3 163. Through Defendant's performance, sale, and/or purchase of goods and
4 services, it knew or should have known that it must protect Plaintiff's and Class
5 Members' confidential Personal Information in accordance with Defendant's policies,
6 practices, and applicable law.

7 164. As consideration, Plaintiff and Class Members paid money to Defendant for
8 goods and turned over their valuable Private Information to Defendant. Accordingly,
9 Plaintiff and Class Members bargained with Defendant to securely maintain and store
10 their Private Information.

11 165. Defendant violated these contracts by failing to employ reasonable and
12 adequate security measures to secure Plaintiff's and Class Members' Private Information
13 and by allowing the disclosure of said Private Information for purposes not required or
14 permitted under the contracts or agreements.

15 166. Plaintiff and Class Members have been damaged by Defendant's conduct,
16 including by paying for data and cybersecurity protection that they did not receive, as
17 well as by incurring the harms and injuries arising from the Data Breach now and in the
18 future.

19 **COUNT V**
20 **UNJUST ENRICHMENT**
21 **(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)**

22 167. Plaintiff restates and realleges the allegations in the preceding paragraphs as
23 if fully set forth herein.

24 168. This count is pled in the alternative to Counts III and IV above.

25 169. Plaintiff and Class Members conferred a benefit on Defendant by paying for
26 data and cybersecurity procedures to protect their Private Information that they did not
27 receive.

1 170. Defendant has retained the benefits of its unlawful conduct including the
2 amounts received for data and cybersecurity practices that it did not provide. Due to
3 Defendant's conduct alleged herein, it would be unjust and inequitable under the
4 circumstances for Defendant to be permitted to retain the benefit of their wrongful
5 conduct.

6 171. Plaintiff and Class Members are entitled to full refunds, restitution and/or
7 damages from Defendant and/or an order of this Court proportionally disgorging all
8 profits, benefits, and other compensation obtained by Defendant from its wrongful
9 conduct. If necessary, the establishment of a constructive trust from which the Plaintiff
10 and Class Members may seek restitution or compensation may be created.

11 172. Additionally, Plaintiff and Class Members may not have an adequate
12 remedy at law against Defendant, and accordingly plead this claim for unjust enrichment
13 in addition to or, in the alternative to, other claims pleaded herein.

14 **COUNT VI**
15 **DECLARATORY JUDGMENT**
16 **(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)**

17 173. Plaintiff restates and realleges the allegations in the preceding paragraphs as
18 if fully set forth herein.

19 174. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court
20 is authorized to enter a judgment declaring the rights and legal relations of the parties and
21 grant further necessary relief. Furthermore, the Court has broad authority to restrain acts,
22 such as here, that are tortious and violate the terms of the federal and state statutes
23 described in this Complaint.

24 175. Defendant owes a duty of care to Plaintiff and Class Members which
25 required it to adequately secure Private Information.

26 176. Defendant still possesses Private Information regarding Plaintiff and Class
27 Members.

1 177. Plaintiff alleges that Defendant's data security measures remain inadequate.
2 Furthermore, Plaintiff continues to suffer injury as a result of the compromise of her
3 Private Information, and remains at imminent risk that further compromises of her Private
4 Information will occur in the future.

5 178. Under its authority pursuant to the Declaratory Judgment Act, this Court
6 should enter a judgment declaring, among other things, the following:

- 7 a. Defendant owes a legal duty to secure customers' Private Information and
8 to timely notify customers of a data breach under the common law and
9 Section 5 of the FTCA;
- 10 b. Defendant's existing security measures do not comply with its explicit or
11 implicit contractual obligations and duties of care to provide reasonable
12 security procedures and practices appropriate to the nature of the
13 information to protect customers' Private Information; and
- 14 c. Defendant continues to breach this legal duty by failing to employ
15 reasonable measures to secure customers' Private Information.

16 179. This Court also should issue corresponding prospective injunctive relief
17 requiring Defendant to employ adequate security protocols consistent with law and
18 industry standards to protect customers' Private Information, including the following:

- 19 a. Order Defendant to provide lifetime credit monitoring and identity theft
20 insurance to Plaintiff and Class Members.
- 21 b. Order Defendant to comply with its explicit or implicit contractual
22 obligations and duties of care, Defendant must implement and maintain
23 reasonable security measures, including, but not limited to:
- 24 i. engaging third-party security auditors/penetration testers as well
25 as internal security personnel to conduct testing, including
26 simulated attacks, penetration tests, and audits on Defendant's
27 systems on a periodic basis, and ordering Defendant to promptly
28

- 1 correct any problems or issues detected by such third-party
2 security auditors;
- 3 ii. engaging third-party security auditors and internal personnel to run
4 automated security monitoring;
- 5 iii. auditing, testing, and training its security personnel regarding any
6 new or modified procedures;
- 7 iv. segmenting its user applications by, among other things, creating
8 firewalls and access controls so that if one area is compromised,
9 hackers cannot gain access to other portions of Defendant's
10 systems;
- 11 v. conducting regular database scanning and securing checks;
- 12 vi. routinely and continually conducting internal training and
13 education to inform internal security personnel how to identify and
14 contain a breach when it occurs and what to do in response to a
15 breach;
- 16 vii. meaningfully educating its users about the threats they face as a
17 result of the loss of their Private Information to third parties, as
18 well as the steps they must take to protect themselves.

19 180. If an injunction is not issued, Plaintiff will suffer irreparable injury, and lack
20 an adequate legal remedy, in the event of another data breach at Defendant. The risk of
21 another such breach is real, immediate, and substantial. If another breach at Defendant
22 occurs, Plaintiff will not have an adequate remedy at law because many of the resulting
23 injuries are not readily quantifiable.

24 181. The hardship to Plaintiff if an injunction does not issue exceeds the hardship
25 to Defendant if an injunction is issued, especially considering the Data Breach is the
26 second breach of Defendant's network and systems in less than two years. Therefore,
27 Plaintiff will likely be subjected to substantial identity theft and other damage. On the
28

1 other hand, the cost to Defendant of complying with an injunction by finally employing
2 reasonable prospective data security measures is relatively minimal, and Defendant has
3 a pre-existing legal obligation to employ such measures.

4 182. Issuance of the requested injunction will not disserve the public interest. To
5 the contrary, such an injunction would benefit the public by preventing a subsequent data
6 breach at Defendant, thus eliminating the additional injuries that would result to Plaintiff
7 and customers whose Private Information would be further compromised.

8 **PRAYER FOR RELIEF**

9 WHEREFORE, Plaintiff, on behalf of herself and the Class described above,
10 seeks the following relief:

- 11 a. An order certifying this action as a class action under Fed. R. Civ. P. 23,
12 defining the Class as requested herein, appointing the undersigned as Class
13 Counsel, and finding that Plaintiff is a proper representative of the Class
14 requested herein;
- 15 b. Judgment in favor of Plaintiff and Class Members awarding them
16 appropriate monetary relief, including actual damages, statutory damages,
17 equitable relief, restitution, disgorgement, and statutory costs;
- 18 c. An order providing injunctive and other equitable relief as necessary to
19 protect the interests of the Class as requested herein;
- 20 d. An order instructing Defendant to purchase or provide funds for lifetime
21 credit monitoring and identity theft insurance to Plaintiff and Class
22 Members;
- 23 e. An order requiring Defendant to pay the costs involved in notifying Class
24 Members about the judgment and administering the claims process;
- 25 f. A judgment in favor of Plaintiff and the Class awarding them pre-judgment
26 and post judgment interest, reasonable attorneys' fees, costs and expenses
27 as allowable by law, and
28

1 g. An award of such other and further relief as this Court may deem just and
2 proper.

3 **DEMAND FOR JURY TRIAL**

4 Plaintiff hereby demands trial by jury as to all triable issues.

5
6 Dated: September 11, 2023

Respectfully submitted,

7 By: /s/ Kyle McLean

8 Kyle McLean (SBN #330580)

9 Email: kmclean@sirillp.com

Mason Barney*

10 Email: mbarney@sirillp.com

11 Tyler Bean*

Email: tbean@sirillp.com

12 **SIRI & GLIMSTAD LLP**

700 S. Flower Street, Ste. 1000

13 Los Angeles, CA 90017

14 Telephone: 213-376-3739

15 *Attorneys for Plaintiff and the Proposed Class*

16 **Pro Hac Vice Applications Forthcoming*

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [See Tickets Hit with Class Action Over Months-Long 2023 Data Breach](#)
