John J. Nelson (317598)
Milberg Coleman Bryson Phillips Grossman, PLLC
280 S. Beverly Drive
Beverly Hills, CA 90212
Telephone: (858) 209-6941
Fax: (865) 522-0049
Email: jnelson@milberg.com

Counsel for Plaintiff and the Putative Class

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

CONNOR ROWE, individually and on behalf of all others similarly situated, Plaintiff, v. STERLING VALLEY SYSTEMS INC. d/b/a/ INNTOPIA, a Vermont corporation, Defendants.	Case No.: **CLASS ACTION COMPLAINT FOR:** **1. NEGLIGENCE;** **2. VIOLATION OF THE CALIFORNIA CONSUMER PRIVACY ACT;** **3. VIOLATION OF THE CUSTOMER RECORDS ACT;** **4. VIOLATION OF THE UNLAWFUL AND UNFAIR PRONGS OF THE UCL.** **DEMAND FOR JURY TRIAL**

Plaintiff Connor Rowe ("Plaintiff"), individually and on behalf of himself and all other persons similarly situated, brings this Class Action Complaint against Sterling Valley Systems, Inc. d/b/a Inntopia ("Inntopia" or "Defendant"), and alleges, upon personal knowledge as to his own actions and his counsel's investigation, and upon information and belief as to all other matters, as follows:

JURISDICTION

1. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5,000,000 exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant. Moreover, this Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(a)(1) because Plaintiff is a California citizen and is therefore diverse from Defendant, who is a citizen of Vermont.

2. This Court has personal jurisdiction over Defendant because Defendant has systematic and continuous contacts with the State of California through its website, Defendant collects and maintains the personal information of California residents, Defendant markets and sells it services to and within California, and it transacts with California companies and residents.

VENUE

3. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because Plaintiff resides within this judicial district and because a substantial part of the events giving rise to the claims alleged herein occurred within this judicial district.

PARTIES

4. Plaintiff Connor Rowe ("Plaintiff") is a citizen of California residing in Alameda County, California.

5. Defendant Inntopia, is a corporation organized and existing under the laws of the State of Vermont, with its principal place of business at 782 Mountain Road, Stowe, Vermont, 05672.

NATURE OF THE ACTION

6. This is a data breach class action brought on behalf of consumers whose sensitive personal information was stolen by cybercriminals in a cyber-attack directed at Defendant that began on or around October 9, 2021 and was detected by Inntopia on or around February 18, 2022 (the "Data Breach"). The Data Breach reportedly involved the compromise of sensitive information of at least 17,952 consumers.

7. Information stolen in the Data Breach included individuals' sensitive information, including payment card account numbers. (collectively the "PII").

8. As a result of the Data Breach, Plaintiff and Class Members suffered ascertainable losses in the form of loss of the value of their private and confidential information, loss of the benefit of their contractual bargain, out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

9. Plaintiff's and Class Members' sensitive personal information—which was entrusted to Defendant, its officials, and agents—was compromised, unlawfully accessed, and stolen due to the Data Breach.

10. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Plaintiff's and Class Members' PII that Defendant collected and maintained for its own pecuniary benefit.

11. Defendant maintained the PII in a reckless manner. In particular, the PII was maintained on Defendant's computer network in a condition vulnerable to cyberattacks of this type.

12. Upon information and belief, the mechanism of the cyber-attack and potential for improper disclosure of Plaintiff's and Class Members' PII was a known

and foreseeable risk to Defendant, and Defendant was on notice that failing to take steps necessary to secure the PII from those risks left that property in a dangerous condition.

13. In addition, Defendant and its employees failed to properly monitor the computer network and systems that housed Plaintiff's and the Class Members' PII. Had Defendant properly monitored its property, it would have discovered the intrusion sooner.

14. Because of the Data Breach, Plaintiff and Class Members suffered injury and damages in the form of theft and misuse of their PII.

15. In addition, Plaintiff's and Class Members' identities are now at risk because of Defendant's negligent conduct because the PII that Defendant collected and maintained is now in the hands of data thieves.

16. As a further result of the Data Breach, Plaintiff and Class Members have been exposed to a substantial and present risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

17. Plaintiff and Class Members have and may also incur out-of-pocket costs, e.g., for purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

18. As a direct and proximate result of the Data Breach, Plaintiff and Class Members have suffered and will continue to suffer damages and economic losses in the form of: the loss of time needed to: take appropriate measures to avoid unauthorized and fraudulent charges; change their usernames and passwords on their accounts; investigate, correct and resolve unauthorized debits, charges, and fees charged against their accounts; and deal with spam messages and e-mails received as a result of the Data Breach. Plaintiff and Class Members have likewise suffered and will continue to suffer an invasion of their property interest in their own PII such that they are entitled to damages for unauthorized access to and misuse of their PII

from Defendants. Furthermore, Plaintiff and Class Members presently and will continue to suffer from damages associated with the unauthorized use and misuse of their PII as thieves will continue to use the stolen information to obtain money and credit in their name for several years.

19. Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals whose PII was accessed and/or removed from the network during the Data Breach.

20. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendants' data security systems, future annual audits, and adequate credit monitoring and identity restoration services funded by Defendants.

21. Accordingly, Plaintiff brings this action against Defendant seeking to redress its unlawful conduct.

SUBSTANTIVE ALLEGATIONS

Defendants' Background

22. Defendant is a provider of software and e-commerce solutions to the hospitality industry and sells a range of services which include consumer marketing and analytics, business intelligence, booking software, and sales platforms to resorts and hotels across the country.

23. During the relevant time, Defendant operated across the United States and within California.

24. In the ordinary course of Defendant's business it collects, custodies, and maintains the sensitive information of its client's customers, like Plaintiff.

25. On information and belief Defendant gathers and maintains the sensitive PII of consumers like Plaintiff, such as:

a. Name;

b. billing address;

c. shipping address;

d. email address;

e. name on the payment card;

f. type of payment card;

g. full payment card number;

h. payment card expiration date; and

i. security code or CVV code (card verification number).

26. As a condition of transacting with Defendant, Defendant requires its clients to disclose some or all of the Private Information listed above.

27. Plaintiff used Defendant's services when he booked services for Whistler Resort. On May 23, 2022, he received a letter from Defendant entitled "Notice of Data Breach," indicating that it provided the e-commerce software Plaintiff used to make reservations and book services for Whistler Resort and that Defendant had discovered that an intruder had access to the personal information stored in its network between October 2021 and February 2022. The letter further indicated that Plaintiff's PII, which included his payment card information, was exposed by Defendant. This is the same credit card he used to purchase services at Whistler Resort.

28. In the course of collecting the Private Information of consumers, including Plaintiff, Defendant promised to provide confidentiality and adequate security for consumer data through their applicable privacy policy and through other disclosures.[1] Defendant even noted, "technology in the resort industry isn't perfect. But that lack of perfection is no excuse for ecommerce and marketing vendors to take a lazy attitude toward information security."

29. Defendant certainly was aware of the risks associated with collecting and maintaining the PII of consumers, and similarly was aware that data breaches associated with the travel industry were growing in frequency and that the

[1] https://corp.inntopia.com/about-us/security/

consequences were severe.[2] In a self-published article titled "*The cost and frequency of travel data breaches is rising*," Defendant itself proclaimed:

> [Data security is] not just about avoiding bad headlines, it's about proactively avoiding moments that can sink an entire travel business – both financially and with their reputation in the market – and erase decades of work in an instant. Businesses that have put their trust in us to help them grow.

Defendant also recognized the severe consequences of failing to secure consumer PII, noting that the costs resulting from data breaches in 2019 was estimated at $8.19 million in the United States alone.[3]

30. Despite its assurances to protect consumer information and to secure its network, Defendant allowed an intruder access to its network and consumer PII undetected for over months, from October 2021 to February 2022. Had Defendant been properly monitoring its systems and had Defendant implemented proper data security standards and training, this Data Breach never would have happened or would have been detected sooner and allowed Plaintiff and Class members to sooner mitigate the consequences thereof.

The Data Breach

31. Starting in or about May of 2022, Defendant sent customers via mail a "Notice of Data Breach." The notice informed affected customers that Inntopia had detected an intrusion into its systems that began in October of 2021 and was only detected in February of 2022: The intruder managed to access the payment card information of consumers, including Plaintiff and the Class, that Defendant maintained and custodied.

[2] https://corp.inntopia.com/cost-and-frequency-of-travel-data-breaches/

[3] *Id.*

32. Defendant's notice to the state Attorney General also provided this same information.[4]

33. Defendant failed to use encryption to protect sensitive information transmitted online, and unauthorized individuals accessed consumers' PII that Defendant voluntarily collected and maintained for its own pecuniary benefit, including payment card numbers and possibly more.[5][6]

34. It is thus clear that the information exposed in the Data Breach was unencrypted: California law requires companies to notify California residents "whose **unencrypted** personal information was, or is reasonably believed to have been, acquired by an unauthorized person" due to a "breach of the security of the system[.]" Cal. Civ. Code § 1798.82(a)(1) (emphasis added). Defendants notified the California Attorney General of the Data Breach on Dec. 18, 2021, evidencing that the exposed data was unencrypted.

35. In a debit or credit card purchase transaction, card data must flow through multiple systems and parties to be processed. Generally, the cardholder presents a credit or debit card to an e-commerce retailer (through an e-commerce website) to pay for merchandise. The card is then "swiped" and information about the card and the purchase is stored in the retailer's computers and then transmitted to the acquirer or processor (i.e., the retailer's bank). The acquirer relays the transaction information to the payment card company, who then sends the information to the issuer (i.e., cardholder's bank). The issuer then notifies the payment card company of its decision to authorize or reject the transaction.

36. There are two points in the payment process where sensitive cardholder data is at risk of being exposed or stolen: pre-authorization when the merchant has

[4] https://ago.vermont.gov/blog/2022/04/05/inntopia-data-breach-notice-to-consumers/?utm_source=rss&utm_medium=rss&utm_campaign=inntopia-data-breach-notice-to-consumers.

[5] *https://oag.ca.gov/ecrime/databreach/reports/sb24-552326*.

[6] *https://oag.ca.gov/ecrime/databreach/reports/sb24-553641*

captured a consumer's data and it is waiting to be sent to the acquirer; and post-authorization when cardholder data has been sent back to the merchant with the authorization response from the acquirer, and it is placed into some form of storage in the merchant's servers.

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

38. The financial fraud suffered by Plaintiff and other customers demonstrates that Defendant chose not to invest in the technology to encrypt payment card data within its e-commerce software and booking engines to make its customers' data more secure; failed to install updates, patches, and malware protection or to install them in a timely manner to protect against a data security breach; and/or failed to provide sufficient control employee credentials and access to computer systems to prevent a security breach and/or theft of payment card data.

39. As Defendant itself recognizes, theft of PII is gravely serious.[7][8] PII is a valuable property right. Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

40. Moreover, there may be a time lag between when harm occurs versus when it is discovered, and also between when personal information or payment card

[7] https://corp.inntopia.com/cost-and-frequency-of-travel-data-breaches/

[8] https://corp.inntopia.com/about-us/security/

data is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [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 or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[9]

41. PII and financial information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

42. There is a strong probability that entire batches of stolen payment card information have been dumped on the black market or are yet to be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud for many years into the future. Thus, Plaintiff and Class Members must vigilantly monitor their financial accounts for many years to come.

43. Plaintiff and members of the classes defined below have or will suffer actual injury as a direct result of Defendants' Data Breach. In addition to fraudulent charges and damage to their credit, many victims spent substantial time and expense relating to:

- Finding fraudulent charges;
- Canceling and reissuing cards;
- Purchasing credit monitoring and identity theft prevention;
- Addressing their inability to withdraw funds linked to compromised accounts;
- Removing withdrawal and purchase limits on compromised accounts;

[9] "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown" by GAO, June 2007, at: https://www.gao.gov/assets/270/262904.html (last accessed May 24, 2021).

- Taking trips to banks and waiting in line to obtain funds held in limited accounts;
- Spending time on the phone with or at the financial institution to dispute fraudulent charges;
- Resetting automatic billing instructions; and/or
- Paying late fees and declined payment fees imposed as a result of failed automatic payments.

44. Plaintiff and Class Members have been damaged by the compromise of their PII in the Data Breach.

45. Plaintiff's PII was compromised as a direct and proximate result of the Data Breach, and subsequently used for fraudulent transactions.

46. As a direct and proximate result of the Data Breach, Plaintiff's PII was accessed and exfiltrated and is in the hands of identity thieves and criminals, as evidenced by the fraud perpetrated against Plaintiff described below.

47. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered actual fraud.

48. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud. Plaintiff and Class Members now must take the time and effort to mitigate the actual and potential impact of the Data Breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting her financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

49. Plaintiff and Class Members may also incur 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.

50. Plaintiff and Class Members also suffered a loss of value of their PII when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

51. Plaintiff and Class Members were also damaged via benefit-of-the-bargain damages. The implied contractual bargain entered into between Plaintiff Defendant's clients included Defendant's contractual obligation to provide adequate data security, which Defendant failed to provide. Thus, Plaintiff and the Class Members did not get what they paid for.

52. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their financial accounts and records for misuse.

53. Plaintiff and the Class have suffered, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. Trespass, damage to and theft of their personal property including personal information and payment card data;

b. Improper disclosure of their personal information and payment card data;

c. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by customers' personal information and payment card data being placed in the hands of criminals and having been already misused via the sale of such information on the Internet black market;

d. Damages flowing from Defendant's untimely and inadequate notification of the data breach;

e. Loss of privacy suffered as a result of the Data Breach;

f. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;

g. Ascertainable losses in the form of deprivation of the value of customers' personal information for which there is a well-established and quantifiable national and international market; and

h. The loss of use of and access to their account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money customers were permitted to obtain from their accounts.

54. The substantial delay in providing notice of the Data Breach deprived Plaintiff and the Class Members of the ability to promptly mitigate potential adverse consequences resulting from the Data Breach. As a result of Defendants' delay in detecting and notifying consumers of the Data Breach, the risk of fraud for Plaintiff and Class Members was and has been driven even higher.

Plaintiff's Experience

55. Plaintiff Connor Rowe used Defendant's e-commerce software and/or booking engine when he booked services through Whistler Resort. He did so using his Chase credit card. On or about May 23, 2022, Plaintiff received a Notice of Data Breach letter from Defendant indicating that it operates the reservation system for Whistler.com Systems Inc. which was the platform on which Plaintiff paid for services for Whistler Resort.

56. Not only was Plaintiff's PII accessed and exfiltrated from Defendant, but someone also attempted to use his credit card information to make unauthorized charges.

57. Soon after the intrusion into Defendant's system, Plaintiff received a fraud alert indicating that someone was attempting to use his Chase credit card, the same card whose information he entered into Defendant's booking platform, to make unauthorized charges. Due to the same credit card began used, the fact that he had not experienced similar fraud alerts or identity theft incidents, and the proximity of the fraud attempt to the data breach, Plaintiff believes that this unauthorized use resulted from Inntopia's failure to properly secure his data.

58. In response to the Data Breach notice, Plaintiff had to take time out of his day to deal with the ramifications, including contacting his credit card issuer to cancel and reissue his compromised credit card, calls to Experian IdentityWorks to attempt to receive complimentary credit monitoring, and researching the Data Breach Notice, Defendant, and his own credit rating. Plaintiff estimates that he was forced to expend at least five hours of his personal time to deal with the consequences of Defendant's Data Breach. This was time he otherwise would have spent performing other activities, such as his job and/or leisure activities for the enjoyment of life.

59. Knowing that a hacker stole his PII, and that his PII is available for sale on the dark web, has caused Plaintiff great concern. He is now very concerned about credit card theft and identity theft in general. This breach has given Plaintiff hesitation about shopping on or engaging with other online websites.

60. Now, due to Defendant's misconduct and the resulting Data Breach, hackers obtained his PII at no compensation to Plaintiff whatsoever. That is money lost for him, and money gained for the hackers–who could sell his PII on the dark web.

61. Moreover, Plaintiff suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of criminals.

62. Plaintiff also paid a premium to Whistler Resort, with whom Defendant contracted, and part of that premium was intended to apply towards Defendant's costs for data security but was not so applied.

63. Plaintiff has a continuing interest in ensuring his PII, which remains in Defendant's possession, is protected and safeguarded from future breaches, or from the same or similar mechanism of attack, which is exploits a vulnerability in Defendant's data security. On information and belief this and other vulnerabilities remain.

Plaintiff's Efforts to Secure PII

64. Defendant's Data Breach caused Plaintiff harm.

65. Prior to the activity described above during the period in which the Data Breach occurred, the credit card that Plaintiff used to purchase products from the companies Defendant contracted with had never been stolen or compromised. Plaintiff regularly reviewed his credit accounts and other financial statements routinely and to his knowledge this card had not been compromised in any manner.

66. Additionally, Plaintiff never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

67. Plaintiff stores any and all electronic documents containing his PII in a safe and secure location, and shreds any documents he receives in the mail that contain any of his PII, or that may contain any information that could otherwise be used to compromise his credit card.

CLASS ACTION ALLEGATIONS

68. Plaintiff brings this nationwide class action pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure, on behalf of himself and on behalf of all members of the following class:

> All individuals whose PII was compromised in the data breach discovered by Defendant on or about February 18, 2022 (the "Class").

69. Plaintiff also seeks certification of a California sub-class defined as follows:

> All individuals residing in the State of California whose PII was compromised in the data breach discovered by Defendant on or about February 18, 2022 (the "California Subclass").

70. Collectively the Class and the California Subclass are referred to as the "Classes."

71. Excluded from the Classes are the following individuals and/or entities: Defendants and its parents, subsidiaries, affiliates, officers and directors, current or former employees, and any entity in which Defendants have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

72. Plaintiff reserves the right to modify or amend the definitions of the proposed Classes before the Court determines whether certification is appropriate.

73. **Numerosity**: The Classes are so numerous that joinder of all members is impracticable. Defendants have identified at least 17,952 customers whose PII may have been improperly accessed in the data breach, and the Classes are apparently identifiable within Defendants' records.

74. **Commonality**: Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

a. When Defendants actually learned of the data breach and whether the response was adequate;

b. Whether Defendants owed a duty to the Classes to exercise due care in collecting, storing, safeguarding and/or obtaining their PII;

c. Whether Defendants breached that duty;

d. Whether Defendants implemented and maintained reasonable security procedures and practices appropriate to the nature of storing Plaintiff's and Class Members' PII;

e. Whether Defendants acted negligently in connection with the monitoring and/or protection of Plaintiff's and Class Members' PII;

f. Whether Defendants knew or should have known that it did not employ reasonable measures to keep Plaintiff's and Class Members' PII secure and prevent loss or misuse of that PII;

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

h. Whether Defendants caused Plaintiff's and Class Members' damages;

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

j. Whether Plaintiff and the other Class Members are entitled to credit monitoring and other monetary relief;

75. **Typicality**: Plaintiff's claims are typical of those of other Class Members because all had their PII compromised as a result of the Data Breach, due to Defendants' misfeasance.

76. **Adequacy**: Plaintiff will fairly and adequately represent and protect the interests of the Class Members. Plaintiff's counsel are competent and experienced in litigating privacy-related class actions.

77. **Superiority and Manageability**: Under Rule 23(b)(3), a class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the Classes is impracticable. Individual damages for any individual Class Members are likely to be insufficient to justify the cost of individual litigation, so that in the absence of class treatment, Defendants' misconduct would go unpunished. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

78. Class certification is also appropriate under Fed. R. Civ. P. 23(a) and (b)(2) because Defendants have acted or refused to act on grounds generally

applicable to the Classes, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Classes as a whole.

79. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendants owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

b. Whether Defendants breached a legal duty to Plaintiff and the Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

c. Whether Defendants failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach; and

e. Whether Class Members are entitled to actual damages, credit monitoring and/or other injunctive relief as a result of Defendants' wrongful conduct.

COUNT I

Negligence

(On Behalf of Plaintiff and the Class)

80. Plaintiff re-alleges and incorporates by reference the allegations contained in the preceding paragraphs.

81. Plaintiff brings this Count on his own behalf and that of the Class.

82. Defendant owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, using, and protecting their PII from unauthorized third parties.

83. The legal duties owed by Defendant to Plaintiff and Class Members include, but are not limited to the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII of Plaintiff and Class Members in its possession;

b. To protect PII of Plaintiff and Class Members in their possession using reasonable and adequate security procedures that are compliant with industry-standard practices; and

c. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches, including promptly notifying Plaintiff and Class Members of the Data Breach.

84. Defendant's duty to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interested and enforced by the FTC, the unfair practices of failing to use reasonable measures to protect PII by companies such as Defendants.

85. Various FTC publications and data security breach orders further form the basis of Defendant's duty. Plaintiff and Class Members are consumers under the FTC Act. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with industry standards.

86. Defendant also had a duty to use reasonable security measures under the California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 *et seq*. Defendant failed to satisfy that duty resulting in the harm identified herein.

87. Defendant similarly had a duty to immediately notice California consumers of the Data Breach under the California Customer Records Act, Cal. Civ. Code §§ 1798.80 *et seq*. Defendant failed to satisfy that duty resulting in the harm identified herein.

88. Defendant breached its duties to Plaintiff and Class Members. Defendant knew or should have known the risks of collecting and storing PII and the importance of maintaining secure systems.

89. Defendant knew or should have known that their security practices did not adequately safeguard Plaintiff's and the other Class Members' PII, including, but not limited to, the failure to detect the data breach the moment it happened.

90. Through Defendant's acts and omissions described in this Complaint, including Defendants' failure to provide adequate security and its failure to protect the PII of Plaintiff and the Class from being foreseeably captured, accessed, exfiltrated, stolen, disclosed, accessed, and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure Plaintiff's and Class Members' PII during the period when it was within Defendant's possession and control.

91. Defendant breached the duties it owed to Plaintiff and Class Members in several ways, including:

a. Failing to implement adequate security systems, protocols, and practices sufficient to protect customers' PII and thereby creating a foreseeable risk of harm;

b. Failing to comply with the minimum industry data security standards during the period of the data breach (e.g., There is no indication that Defendant encrypts customers' order information, such as name, address, and credit card number, during data transmission, which did not occur here);

c. Failing to act despite knowing or having reason to know that Defendant's systems was vulnerable to a data breach (e.g., Defendant did not detect the Data Breach for over four months); and

d. Failing to timely and accurately disclose to customers that their PII had been improperly acquired or accessed and was potentially available for

sale to criminals on the dark web (e.g., more than two months went by before Defendant notified customers of the Data Breach).

92. Due to Defendants' conduct, Plaintiff and Class Members are entitled to credit monitoring. Ongoing credit monitoring is reasonable here. The PII taken can be used towards identity theft and other types of financial fraud against the Class Members. Hackers not only stole many consumers' PII, they also sold or attempted to use the PII themselves as indicated by the fraud alert received by Plaintiff. There is no question that this PII was taken by sophisticated cybercriminals, increasing the risks to the Class Members. The consequences of identity theft are serious and long-lasting. There is a benefit to early detection and monitoring.

93. Some experts recommend that data breach victims obtain credit monitoring services for at least ten years following a data breach. Annual subscriptions for credit monitoring plans range from approximately $219 to $358 per year.

94. As a result of Defendant's negligence, Plaintiff and Class Members suffered injuries that include: (i) the lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the data breach, including but not limited to time spent cancelling and reissuing credit cards believed to be associated with the compromised account; (iv) the continued risk to their PII, which may remain for sale on the dark web and is in Defendants' possession, subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect the PII of consumers in their continued possession; and (v) future costs in terms of time, effort, and money that will be expended to prevent, monitor, detect, contest, and repair the impact of the PII compromised as a result of the data breach for the remainder of the lives of Plaintiff and Class Members, including ongoing credit monitoring.

95. These injuries were reasonably foreseeable given the history of security breaches of this nature. The injury and harm that Plaintiff and the other Class Members suffered was the direct and proximate result of Defendants' negligent conduct.

COUNT II

Violation of California Consumer Privacy Act

Cal. Civ. Code §§ 1798.100 *et seq.*

(On Behalf of Plaintiff and the California Subclass)

96. Plaintiff re-alleges and incorporates by reference the allegations contained in the preceding paragraphs.

97. Plaintiff brings this Count on his own behalf and that of the California Subclass (the "Class" as used in this Count).

98. California law requires that a business that owns, licenses, or maintains personal information about a California resident must implement and maintain reasonable security procedures and practices to protect the information from unauthorized access, destruction, use, modification, or disclosure. Cal. Civ. Code § 1798.81.5(b).

99. Plaintiff is a California resident and a consumer as defined by Cal. Civ. Code § 1798.140(g).

100. Defendant is a "business" as defined by Cal. Civ. Code § 1798.140(c) because it is a for-profit limited liability company based and doing business in California that "collects consumers' personal information or on the behalf of which that information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information."

101. Additionally, Defendant meets one or more of the thresholds established in Cal. Civ. Code § 1798.140(c)(1)(A)-(C).

102. Alternatively, Defendant is controlled by a business as defined in Cal. Civ. Code § 1798.140(c)(1) and that shares common branding with the business.

103. Defendant stored or maintained Plaintiff's and Class Members' personal information, as defined by Cal. Civ. Code § 1798.81.5(d)(1), in nonencrypted or nonredacted form allowing unauthorized malicious threat actors to access and exfiltrate, steal or disclose the data during the Data Breach described above.

104. Defendant failed to implement and maintain numerous basic, foundational, and organizational critical security controls, including, but not limited to, managing cyber vulnerabilities on an ongoing basis, maintaining secure configurations and settings for hardware and software; collecting, managing, and analyzing IT event logs; using strong encryption and data loss prevention software; using automated tools at perimeters to monitor for sensitive data leaving the network and blocking unauthorized attempts to exfiltrate it; and adequately training its personnel in cybersecurity practices.

105. Defendant's failure to implement these controls and other industry-standard practices constitutes a violation of Defendant's duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect personal information.

106. As a result, of Defendant's cybersecurity failures, unauthorized parties exploited vulnerabilities and weaknesses in Defendant's information security and gained unauthorized access to Plaintiff's and Class Members' personal information.

107. The Data Breach occurred as a direct result of Defendant's failure to implement and maintain reasonable security procedures and practices to protect Plaintiff's and Class Members' personal information from unauthorized access, destruction, use, modification, or disclosure.

108. Consistent with Cal. Civ. Code § 1798.150(b)(1), Plaintiff provided written notice to Defendant identifying the CCPA provisions Defendant violated.

109. If Defendant is unable to cure or does not cure the violation within 30 days, Plaintiff will amend this complaint to pursue actual or statutory damages as permitted by Cal. Civ. Code § 1798.150(a)(1)(A).

110. Plaintiff presently seeks injunctive and declaratory relief, and any other relief as deemed appropriate by the Court, for Defendant's CCPA violations.

COUNT III

Violation of Duty to Disclose Breach of Security, Customer Records Act

Cal. Civ. Code §§ 1798.80 *et seq.*

(On Behalf of Plaintiff and the California Subclass)

111. Plaintiff re-alleges and incorporates by reference the allegations contained in the preceding paragraphs.

112. Section 1798.2 of the California Civil Code requires any "person or business that conducts business in California, and that owns or licenses computerized data that includes personal information" to disclose a data breach after discovering one "in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, . . . or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system." Cal. Civ. Code § 1798.82.

113. Defendant is company conducting business in California that owns, maintains or licenses computerized data that includes "personal information" as that term is defined in Cal. Civ. Code § 1798.82(h).

114. The Data Breach described in this complaint constitutes a "breach of the security system" of Defendant.

115. As alleged above, Defendant failed to disclose the Data Breach "in the most expedient time possible and without unreasonable delay" when it waited 7 months between discovering the Data Breach and informing Plaintiff and the Class Members about the Data Breach.

116. Defendant began notifying law enforcement agencies on the same day that it began mailing letters to Plaintiff and Class Members: on or around April 22, 2022.

117. Therefore, Defendant's decision to wait two months before beginning to notify Plaintiff and the Class was not because a law enforcement agency advised Defendant that the notification would impede a criminal investigation.

118. Moreover, upon information and belief, Defendant's two-month delay is not explained by Defendant's need to take measures to determine the breach's scope and restore the integrity of the data system.

119. Instead, Defendant's ongoing business interests gave Defendant an incentive to conceal the Data Breach from the public to ensure continued revenue and delay reputational risks.

120. Furthermore, the Notice of Data Incident does not satisfy the requirements of Cal. Civ. Code § 1798.82 because it does not state whether notification was delayed as a result of a law enforcement investigation.

121. As a result of Defendant's violation of Cal. Civ. Code § 1798.82, Plaintiff and Class Members were deprived of prompt notice of the Data Breach and were thus prevented from taking appropriate protective measures, such as securing identity theft protection or requesting a credit freeze. These measures could have prevented some of the damages suffered by Plaintiff and Class Members because their stolen information would have had less value to identity thieves.

122. As a result of Defendant's violation of Cal. Civ. Code § 1798.82, Plaintiff and Class Members suffered incrementally increased damages separate and distinct from those simply caused by the Data Breach itself.

123. Plaintiff and Class Members seek all remedies available under Cal. Civ. Code § 1798.84, including, but not limited to the damages suffered by Plaintiff and Class Members as alleged above and equitable relief.

COUNT IV

Violation of California's Unfair Competition Law

Cal. Bus. & Prof. Code § 17200

(On Behalf of Plaintiff and the California Subclass)

124. Plaintiff re-alleges and incorporates by reference the allegations contained in the preceding paragraphs.

125. Plaintiff brings this Count on his own behalf and that of the California Subclass (the "Class" as used in this Count).

126. By reason of the conduct alleged herein, Defendant engaged in unlawful "business practices" within the meaning of the UCL.

127. Defendant stored patient and customer data of Plaintiff and the Class Members in its computer systems.

128. Plaintiff and Class Members were entitled to assume and did assume Defendant would take appropriate measures to keep their Private Information safe. Defendant did not disclose at any time that Plaintiff's Private Information was vulnerable to hackers because Defendant's data security measures were inadequate and outdated, and Defendant was the only entity in possession of that material information, which it had a duty to disclose. Defendant violated the UCL by failing to implement reasonable and appropriate security measures or follow industry standards for data security, failing to comply with its own posted privacy policies, and by failing to immediately notify Plaintiff and Class Members of the Data Breach. If Defendant had complied with these legal requirements, Plaintiff and Class Members would not have suffered the damages related to the Data Breach, and consequently from, Defendant's failure to timely notify Plaintiff and the Class Members of the Data Breach.

129. Defendant's acts, omissions, and misrepresentations as alleged herein were unlawful and in violation of, inter alia: Section 5(a) of the Federal Trade Commission Act; and the California Consumer Privacy Act, Cal. Civ. Code §§

1798.100 *et seq*; and the California Customer Records Act, Cal. Civ. Code §§ 1798.80 *et seq.*

130. Plaintiff and Class Members suffered injury in fact and lost money or property as the result of Defendant's unlawful business practices. In particular, Plaintiff and Class Members have suffered from improper or fraudulent charges to their credit/debit card accounts; and other similar harm, all as a result of the Data Breach. In addition, their Private Information was taken and is in the hands of those who will use it for their own advantage, or is being sold for value, making it clear that the hacked information is of tangible value. Plaintiff and Class Members have also suffered consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

131. Defendant engaged in unfair acts and practices by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiff's and Class Members' Personal Information with knowledge that the information would not be adequately protected; and by storing Plaintiffs' and Class Members Personal Information in an unsecure electronic environment. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiff and Class Members. They were likely to deceive the public into believing their Personal Information was securely stored when it was not. The harm these practices caused to Plaintiff and Class Members outweighed their utility, if any.

132. Defendant engaged in unfair acts and practices with respect to the provision of services by failing to take proper action following the data breach to enact adequate privacy and security measures and protect Plaintiff's and Class Members Personal Information from further unauthorized disclosure, release, data breaches, and theft. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiff

and Class Members. They were likely to deceive the public into believing their Personal Information was securely stored, when it was not. The harm these practices caused to Plaintiff and Class Members outweighed their utility, if any.

133. As a direct and proximate result of Defendant's acts of unfair practices, Plaintiff and Class Members were injured and lost money or property, including but not limited to the price received by Defendant for the services, the loss of Plaintiff's and Class Members legally protected interest in the confidentiality and privacy of their Personal Information, nominal damages, and additional losses as described above.

134. As a result of Defendant's unlawful and unfair business practices, violations of the UCL, Plaintiff and the Class Members are entitled to injunctive relief, including restitution and all other remedies allowed by law.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all of the members of the Class, respectfully requests that the Court enter judgment in their favor and against Defendants as follows:

A. For an Order certifying the Class as defined herein and appointing Plaintiff and his Counsel to represent the Class;

B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PII;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

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

iii. requiring Defendants to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personal identifying information of Plaintiff and Class Members' PII;

v. prohibiting Defendants from maintaining Plaintiff's and Class Members' PII on a cloud-based database;

vi. requiring Defendants to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendants to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' network is compromised, hackers cannot gain access to other portions of Defendants' systems;

x. requiring Defendants to conduct regular database scanning and securing checks;

xi. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PII, as well as protecting the personal identifying information of Plaintiff and Class Members;

xii. requiring Defendants to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendants to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendants' policies, programs, and systems for protecting PII;

xiv. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendants to meaningfully educate all class members about the threats that they face as a result of the loss of their confidential PII to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants' servers; and

xvii. for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendants' compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For restitution and disgorgement of the revenues wrongfully obtained as a result of Defendants' wrongful conduct;

E. For an award of actual damages and compensatory damages, in an amount to be determined at trial;

F. For an award of costs of suit, litigation expenses and attorneys' fees, as allowable by law; and

G. For such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of himself and all others similarly situated, hereby demands a jury trial for all claims so triable.

Dated: June 20, 2022

/s/ *John J. Nelson*

John J. Nelson (SBN 317598)
Milberg Coleman Bryson Phillips Grossman, Pllc
280 S. Beverly Drive
Beverly Hills, CA 90212
Telephone: (858) 209-6941
Fax: (865) 522-0049
Email: jnelson@milberg.com

Counsel for Plaintiff and the Putative Class

ClassAction.org
