CLARKSON LAW FIRM, P.C.
Ryan J. Clarkson (SBN 257074)
rclarkson@clarksonlawfirm.com
Yana Hart (SBN 306499)
yhart@clarksonlawfirm.com
Tiara Avaness (SBN 343928)
tavaness@clarksonlawfirm.com
22525 Pacific Coast Highway
Malibu, CA 90265
Tel: (213) 788-4050
Fax: (213) 788-4070

NUSSBAUM LAW GROUP, P.C.
Linda P. Nussbaum *(PHV Application forthcoming)*
lnussbaum@nussbaumpc.com
1133 Avenue of the Americas, 31st Floor
New York, NY 10036
Tel: (917) 438-9189

Attorneys for Plaintiff and the Proposed Class

[Additional Counsel on Signature Page]

IN THE UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

ANDREA BURNS, on her own behalf and on behalf of all others similarly situated,

Plaintiff,

v.

TICKETMASTER, LLC and LIVE NATION ENTERTAINMENT, INC.,

Defendants.

Case No. 2:24-cv-4674

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

CLASS ACTION COMPLAINT

Plaintiff Andrea Burns ("Plaintiff"), individually and on behalf of all others similarly situated, brings this Class Action Complaint (the "Complaint"), and allege the following against Defendant Live Nation Entertainment, Inc. ("Live Nation"), and Defendant Ticketmaster, LLC ("Ticketmaster") (collectively, "Defendants"), based upon personal knowledge with respect to herself and upon information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters.

NATURE OF THE ACTION

1. This class action arises out of Defendants failure to properly secure and safeguard Plaintiff's and other similar situated individuals' personal identifiable information ("PII"), including "names, addresses, phone numbers, and partial credit card details."[1]

2. Defendants are among the largest producers of live music concerts and live entertainment ticketing sales and marketing companies in the world with 2023 revenues of almost $23 billion.[2]

3. Defendants claim that "[w]e take steps to try to make sure your information is protected and to delete it securely when we no longer need it."[3]

4. Despite these assurances, Defendants failed to adequately safeguard Plaintiff's and Class Members' highly sensitive Private Information that it collected and maintained.

---

[1] https://www.cbsnews.com/news/ticketmaster-breach-shinyhunters-560-million-customers/ (last accessed Jun. 3, 2024).

[2] https://variety.com/2024/music/news/live-nation-2023-earnings-record-year-1235919844/ (last accessed Jun. 3, 2024).

[3] https://help.livenation.com/hc/en-us/articles/10464047306641-Live-Nation-Entertainment-Privacy-Policy#security (last accessed Jun. 3, 2024).

5. On or about May 20, 2024, Defendants suffered a data breach within a third-party cloud database environment containing company data.[4]

6. In this targeted cyberattack, the infamous cybercrime group known as ShinyHunters, gained access to Defendants' computer systems and data, resulting in the compromise of highly sensitive PII of more than 500 million Ticketmaster customers (the "Data Breach").[5]

7. As a result of the Data Breach, Plaintiff and Class Members suffered ascertainable losses in the form of the benefit of their bargain, out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the attack, emotional distress, and the imminent risk of future harm caused by the compromise of their PII.

8. On or around May 28, 2024, CyberDaily, an Australian-based news outlet that delivers breaking news, market intelligence and insights for Australia's cyber sector first reported the Data Breach, stating that hackers posted the "price tag" for PII on a dark web forum.[6]

9. This was not a passive data breach where, for example, it is unclear whether the compromised data was targeted or even seen. Here, the Data Breach occurred as a result of an unauthorized third-party gaining access to and obtaining Defendants'

---

[4] Live Nation Entertainment, Inc., Form 8-K (May 31, 2024), *available at* https://www.sec.gov/Archives/edgar/data/1335258/000133525824000081/lyv-20240520.htm.

[5] https://thehill.com/homenews/nexstar_media_wire/4692567-ticketmaster-data-breach-hackers-claim-over-500-million-users-compromised/ (last accessed Jun. 3, 2024); https://www.nytimes.com/2024/05/31/business/ticketmaster-hack-data-breach.html (last accessed Jun. 3, 2024).

[6] https://www.cyberdaily.au/security/10632-hackers-claim-ticketmaster-live-nation-data-breach-more-than-500m-compromised (last accessed Jun. 3, 2024).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

customers' PII from internal computer systems.[7]

10. The Data Breach was a direct result of Defendants' failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect Personal Information from the foreseeable threat of a cyberattack.

11. By being entrusted with Plaintiff's and Class members' PII for their own pecuniary benefit, Defendants assumed a duty to Plaintiff and Class Members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard Plaintiff's and Class Members' PII against unauthorized access and disclosure.

12. Defendants also had a duty to adequately safeguard this PII under controlling case law, as well as pursuant to industry standards and duties imposed by statutes, including Section 5 of the Federal Trade Commission Act (the "FTC Act").

13. Defendants breached those duties by, among other things, failing to implement and maintain reasonable security procedures and practices to protect the PII in its possession from unauthorized access and disclosure.

14. As a result of Defendants' inadequate security and breach of its duties and obligations, the Data Breach occurred, and Plaintiff and Class Members suffered injury and ascertainable losses in the form of out-of-pocket expenses, loss of value of their time reasonably incurred to remedy or mitigate the effects of the attack, the diminution in value of their personal information from their exposure, and the present and imminent threat of fraud and identity theft. This action seeks to remedy these failings and their consequences.

15. Despite having been accessed and exfiltrated by unauthorized criminal actors, Plaintiff's and Class Members' sensitive and confidential PII remains in Defendants' possession. Absent additional safeguards and independent review and oversight, the

[7] https://www.abc.net.au/news/2024-05-30/ticketmaster-data-breach-how-to-check-if-you-have-been-hacked/103912494 (last accessed Jun. 3, 2024).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

information remains vulnerable to further cyberattacks and theft.

16. Defendants disregarded the rights of Plaintiff and Class Members by, *inter alia*, failing to take adequate and reasonable measures to ensure their data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard PII; failing to take standard and reasonably available steps to prevent the Data Breach; failing to properly train its staff and employees on proper security measures; and failing to provide Plaintiff and Class Members prompt and adequate notice of the Data Breach.

17. In addition, Defendants failed to properly monitor the computer network and systems that housed the PII. Had Defendants properly monitored these electronic systems, Defendants would have discovered the intrusion sooner or prevented it altogether.

18. The security of Plaintiff's and Class Members' identities is now at substantial risk because of Defendants' wrongful conduct as the PII that Defendants collected and maintained is now in the hands of data thieves. This present risk will continue for the course of their lives.

19. Armed with the PII accessed in the Data Breach, data thieves can commit a wide range of crimes.

20. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a present and imminent risk of fraud and identity theft. Among other measures, Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft. Further, Plaintiff and Class Members will incur out-of-pocket costs to purchase adequate credit monitoring and identity theft protection and insurance services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

21. The Private Information compromised in the Data Breach includes: the identifying information of 560 million Ticketmaster customers, including credit card

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

numbers and ticket sales.[8]

22. As a result of Defendants' actions, Plaintiffs and the Class Members experienced damages from: (i) theft of their Personal Information and the resulting loss of privacy rights in that information; (ii) improper disclosure of their Personal Information; (iii) loss of value of their Personal Information; (iv) the amount of ongoing reasonable identity defense and credit monitoring services made necessary as mitigation measures; (v) Defendants' retention of profits attributable to Plaintiffs' and other customers' Personal Information that Defendants failed to adequately protect; (vi) economic and non-economic impacts that flow from imminent, and ongoing threat of fraud and identity theft to which Plaintiffs are now exposed to; (vii) ascertainable out-of-pocket expenses and the value of their time allocated to fixing or mitigating the effects of this data breach; and (viii) overpayments of Defendants' products and/or services which Plaintiffs purchased.

23. Accordingly, Plaintiff brings this action against Defendants, seeking redress for Defendants' unlawful conduct and asserting claims for: (i) negligence; (ii) negligence per se; (iii) breach of fiduciary duty; (iv) unjust enrichment; and (v) breach of implied contract. Through these claims, Plaintiff seeks damages in an amount to be proven at trial, as well as injunctive and other equitable relief, including improvements to Defendants' data security systems, policies, and practices, future annual audits, and adequate credit monitoring services funded by Defendants.

JURISDICTION AND VENUE

24. This Court has original subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2), because: (i) the amount in controversy exceeds $5 million, exclusive of interest and costs; (ii) the number of class

[8] *https://www.nytimes.com/2024/05/31/business/ticketmaster-hack-data-breach.html* (last accessed Jun. 3, 2024).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

members exceeds 100 and (iii) minimal diversity exists because many class members, including Plaintiff, have different citizenships from Defendants.

25. This Court has personal jurisdiction over Defendants because Defendants have purposefully availed themselves of the laws, rights, and benefits of the State of California. Defendants are headquartered in California and have engaged in activities including (i) directly and/or through its parent companies, affiliates and/or agents providing services throughout the United States in this judicial district; (ii) conducting substantial business in this forum; and/or (iii) engaging in other persistent courses of conduct and/or deriving substantial revenue from services provided in California and in this judicial District.

26. This Court has supplemental jurisdiction to hear all state law statutory and common law claims pursuant to 28 U.S.C. § 1367.

27. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District. Moreover, Defendants are based in this District, maintain Plaintiff's and Class Members' Private Information in this District, and has caused harm to Plaintiff and Class Members in this District.

PARTIES

Plaintiff Andrea Burns

28. At all relevant times, Plaintiff Andrea Burns ("Plaintiff") is and has been a citizen of the State of Florida.

29. Plaintiff created an account on Defendants' Ticketmaster/LiveNation website in or around 2017 to purchase event tickets. Plaintiff provided her PII to Defendants when opening her account.

30. Since opening her account, Plaintiff has made at least three event ticket purchases using her Ticketmaster/LiveNation website account.

31. Plaintiff's account with Defendants remains active.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

32. Plaintiff is deeply concerned about the Data Breach because she frequently uses Ticketmaster to purchase event tickets. Plaintiff continues to worry about her Private Information, as it is readily available for cybercriminals to sell, buy, and exchange, on the Dark Web.

33. Since learning about the Data Breach, Plaintiff spent several hours researching the data breach to determine the extent and gravity of the Data Breach and anticipates needing to spend substantial additional time to monitor the effects on her credit and bank accounts, as well as mitigate damages. Plaintiff will need to review for fraudulent activity and closely monitor her financial information.

34. Plaintiff has a continuing interest in ensuring that her Private Information, which remains in Defendants' possession, is protected, and safeguarded from future breaches.

Defendant Ticketmaster, LLC

35. Defendant Ticketmaster, LLC ("Ticketmaster") is a wholly owned subsidiary of Defendant Live Nation Entertainment, Inc.

36. Ticketmaster is a limited liability company organized and existing under the laws of Virginia with its principal place of business in Hollywood, California. 41. Ticketmaster is the largest ticketing company in the United States, with 2022 revenue of Approximately $16.7 billion.[9]

37. Plaintiff and Class Members are current and former customers of Ticketmaster and account holders on Ticketmaster.com.

38. Due to the nature of the services Ticketmaster provides, it receives and is entrusted with securely storing customers' Private Information, which includes, inter alia, individuals' full name, payment information, occasional location data, and other sensitive

[9] https://www.zippia.com/ticketmaster-careers-41797/revenue/ (last accessed Jun. 3, 2024).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

information.

39. Ticketmaster promised to provide confidentiality and adequate security for the data it collected from customers through its applicable privacy policy and through other disclosures in compliance with statutory privacy requirements.

Defendant Live Nation Entertainment, Inc.

40. Defendant Live Nation Entertainment, Inc. ("Live Nation") is a Delaware corporation with its principal place of business in Beverly Hills, California.

41. Live Nation is the largest entertainment company in the world, connecting over half a billion fans across all its platforms in 29 countries.

FACTUAL ALLEGATIONS

A. The Data Breach, Defendants' Unsecure Data Management, and Disclosure of Data Breach

42. On or about May 20, 2024, Defendants suffered a data breach within a third-party cloud database environment containing company data.[10]

43. On or around May 28, 2024, CyberDaily, an Australian-based tech outlet first reported that the infamous cybercrime group called ShinyHunters posted on the dark web, a price tag for the PII it unlawfully obtained from Defendants.[11]

44. On or around May 28, 2024, it was subsequently reported that the Private Information of 560,000,000 Ticketmaster customers were compromised and listed for sale.[12]

---

[10] Live Nation Entertainment, Inc., Form 8-K (May 20, 2024), *available at* https://www.sec.gov/Archives/edgar/data/1335258/000133525824000081/lyv-20240520.htm

[11] https://www.cyberdaily.au/security/10632-hackers-claim-ticketmaster-live-nation-data-breach-more-than-500m-compromised (last accessed Jun. 3, 2024).

[12] https://www.abc.net.au/news/2024-05-29/ticketmaster-hack-allegedlyshinyhunter-customers-data-leaked/103908614 (last accessed Jun. 3, 2024).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

45. On May 31, 2024, Defendants reported the data breach to the Securities and Exchange Commission.[13]

46. Plaintiff and Class Members provided their Private Information to Defendants with the reasonable expectation and mutual understanding that Defendants would comply with its obligations to keep such information confidential and secure from unauthorized access.

47. Data security is purportedly a critical component of Defendants' business model. On a section of Ticketmaster's website, for example, Ticketmaster makes the following statements:

> "Our goal is to maintain your trust and confidence by handling your personal information with respect and putting you in control…As a global company, our fans are located all over the world, depending on your market there are specific laws and regulations around privacy rights such as the GDPR in Europe, LGPD in Brazil and CCPA in United States…We have security measures in place to protect your information."[14]

48. On its website, Defendants also maintain a privacy policy section, stating its compliance with the various international data privacy frameworks and laws of the United States.[15]

49. Contrary to Defendants various express assurances that it would take reasonable measures to safeguard the sensitive information entrusted to it – and only share it for an express authorized persons – an "unauthorized" person or persons was able to access its network servers.

---

[13] Live Nation Entertainment, Inc., Form 8-K (May 31, 2024), *available at* https://www.sec.gov/Archives/edgar/data/1335258/000133525824000081/lyv-20240520.htm.

[14] https://privacy.ticketmaster.com/privacy-policy (last accessed Jun. 3, 2024).

[15] *Id.*; https://help.livenation.com/hc/en-us/articles/10464047306641-Live-Nation-Entertainment-Privacy-Policy (last accessed Jun. 3, 2024).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

50. To date, Defendants have not disclosed specifics of the attack. Plaintiff and Class Members are therefore in the dark, unaware that their Private Information may be used to effectuate identity theft, phishing scams, plunging credit scores and other related cybercrimes.

51. As such, Defendants failed to secure the PII of the individuals that provided them with this sensitive information. They failed to take appropriate steps to protect the PII of Plaintiff and other Class Members from being disclosed.

B. The Data Breach was a Foreseeable Risk of which Defendants Were on Notice

52. Defendants' own conduct created a foreseeable risk of harm to Plaintiff and Class Members. Defendants' misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendants' misconduct also included its decisions not to comply with industry standards for the safekeeping of Plaintiff's and Class Members' PII.

53. As sophisticated business entities handling confidential customer data, Defendants' data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in industries holding significant amounts of Private Information preceding the date of the Data Breach.

54. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding its current and former customers' PII and of the foreseeable consequences that would occur if Defendants' data security system was breached, including, specifically, the significant costs that would be imposed on Defendants' customers as a result of a breach.

55. In light of recent high profile data breaches at other financial services entities, Defendants knew or should have known that their electronic records and consumers' Private Information would be targeted by cybercriminals and ransomware attack groups.

56. Cyberattacks and data breaches of financial services companies are especially

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

problematic because of the potentially permanent disruption they cause to the daily lives of their customers. Stories of identity theft and fraud abound, with hundreds of millions of dollars lost by everyday consumers every year as a result of internet-based identity theft attacks.[16]

57. The U.S. Government Accountability Office ("GAO") released a report on data breaches in 2007 ("GAO Report"), finding that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[17]

58. The FTC recommends that identity theft victims take several steps to protect their personal health and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (and to consider an extended fraud alert that lasts for seven years if identity theft occurs), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[18]

C. The Value of Personal Identifiable Information

59. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[19] Experian

---

[16] Albert Khoury, *Scam alert: 5 most costly data breaches (plus 5 states most targeted)* (July 27, 2022), *available at* https://www.komando.com/security-privacy/most-costly-data-breaches/847800/ (last visited Jun. 3, 2024).

[17] *See* U.S. Gov. Accounting Office, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* ("GAO Report") at 2, GAO (June 2007), https://www.gao.gov/assets/270/262899.pdf [https://perma.cc/GCA5-WYA5].

[18] *Identity Theft Recovery Steps*, FTC, https://www.identitytheft.gov/Steps (last visited Jun. 3, 2024) [https://perma.cc/ME45-5N3A].

[19] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at* https://www.digitaltrends.com/computing/personal-

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[20] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[21]

60. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

61. Moreover, the fraudulent activity resulting from the Data Breach may not come to light for years. There may be a considerable time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), 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.[22]

---

data-sold-on-the-dark-web-how-much-it-costs/#:~:text=To%20gain%20access%20to%20someone's,range%20of%20%2450%20to%20%24200. (last visited Jun. 3, 2024).

[20] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at* https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Jun. 3, 2024).

[21] *In the Dark*, VPNOverview, 2019, *available at* https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Jun. 3, 2024).

[22] *Report to Congressional Requesters,* GAO, at 29 (June 2007), *available at* http://www.gao.gov/new.items/d07737.pdf.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

62. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding its current and former customers' PII and of the foreseeable consequences that would occur if Defendants' data security system was breached, including, specifically, the significant costs that would be imposed on Defendants' customers as a result of a breach.

63. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

64. Defendants were, or should have been, fully aware of the unique type and the significant volume of data in Defendants' possession, amounting to potentially millions of individuals' detailed, personal, finance-related information and thus, the significant number of individuals who would be harmed by a breach of Defendants' data security system.

65. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for its current and former customers' PII.

D. Defendants Failed to Comply with FTC Guidelines

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

67. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

68. In 2016, the FTC updated its publication, Protecting Personal Information: A

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[23] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[24]

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

70. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

71. Defendants failed to properly implement basic data security practices.

72. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to customers' Private Information constitutes an unfair act or

[23] https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last accessed Jun. 3, 2024).

[24] *Id.*

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

73. Defendants were at all times fully aware of the obligation to protect the Private Information of their customers. Defendants were also aware of the significant repercussions that would result from their failure to do so.

E. Plaintiff and the Class Have Suffered Injury as a Result of Defendants' Data Mismanagement

74. As a result of Defendants' failure to implement and follow even the most basic security procedures, Plaintiff's and Class Members' PII have been and are now in the hands of an unauthorized third-party which may include thieves, unknown criminals, banks, credit companies, and other potentially hostile individuals. Plaintiff and other Class Members now face an increased risk of identity theft and will consequentially have to spend, and will continue to spend, significant time and money to protect herself due to Defendants' Data Breach.

75. Plaintiff and other Class Members have had their most personal and sensitive Private Information disseminated to the public at large and have experienced and will continue to experience emotional pain and mental anguish and embarrassment.

76. Plaintiff and Class Members face an increased risk of identity theft, phishing attacks, and related cybercrimes because of the Data Breach. Those impacted are under heightened and prolonged anxiety and fear, as they will be at risk of falling victim to cybercrimes for years to come.

77. PII is a valuable property right.[25] The value of PII as a commodity is measurable. "Firms are now able to attain significant market valuations by employing

[25] *See* Marc van Lieshout, The Value of Personal Data, 457 IFIP Advances in Information and Communication Technology (May 2015), https://www.researchgate.net/publication/283668023 ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible...") (last accessed Jun. 3, 2024).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[26] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[27] It is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

78. As a result of its real value and the recent large-scale data breaches, identity thieves and cyber criminals have openly posted credit card numbers, Social Security numbers, PII, and other sensitive information directly on various Internet websites, making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be aggregated, and become more valuable to thieves and more damaging to victims.

79. Consumers place a high value on the privacy of that data. Researchers shed light on how many consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[28]

80. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

---

[26] *See* Robert Lowes, Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market, Medscape (Apr. 28, 2014), http://www.medscape.com/viewarticle/824192 (last accessed Jun. 3, 2024).

[27] U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017, Interactive Advertising Bureau (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/ (last accessed Jun. 3, 2024).

[28] Janice Y. Tsai et al., The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study, 22(2) Information Systems Research 254 (June 2011), accessible at https://www.jstor.org/stable/23015560?seq=1 (last accessed Jun. 3, 2024).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

81. Plaintiff and members of the Class must immediately devote time, energy, and money to: 1) closely monitor their bills, records, and credit and financial accounts; 2) change login and password information on any sensitive account even more frequently than they already do; 3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and 4) search for suitable identity theft protection and credit monitoring services and pay to procure them. Once PII is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff and Class Members will need to maintain these heightened measures for years, and possibly their entire lives, because of Defendants' conduct. Further, the value of Plaintiff's and Class Members' Private Information has been diminished by its exposure in the Data Breach.

82. As a result of Defendants' failures, Plaintiff and Class Members are at substantial risk of suffering identity theft and fraud or misuse of their Private Information.

83. Plaintiff and Class Members suffered actual injury from having PII compromised as a result of Defendants' negligent data management and resulting Data Breach including, but not limited to (a) damage to and diminution in the value of their PII, a form of property that Defendants obtained from Plaintiff and Class Members; (b) violation of their privacy rights; and (c) present and increased risk arising from the identity theft and fraud.

84. For the reasons mentioned above, Defendants' conduct, which allowed the Data Breach to occur, caused Plaintiff and Class Members these significant injuries and harm.

85. Plaintiff brings this class action against Defendants for their failure to properly secure and safeguard Private Information and for failing to provide timely, accurate, and adequate notice to Plaintiff and other Class Members that their Private Information had been compromised.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

86. Plaintiff, individually and on behalf of all other similarly situated individuals, alleges claims in negligence, negligence per se, breach of implied contract, breach of fiduciary duty, unjust enrichment, and violations of the Florida Deceptive And Unfair Trade Practices Act.

CLASS ACTION ALLEGATIONS

87. Plaintiff brings this action on behalf of herself and on behalf of all other persons similarly situated ("the Class").

88. Plaintiff proposes the following Class and Subclass definitions, subject to amendment(s) as appropriate:

Nationwide Class

> All individuals residing in the United States whose Private Information was compromised as a result of the Data Breach, including all individuals who were sent a notice of the Data Breach ("the Class").

Florida Subclass

> All individuals identified by Defendant (or its agents or affiliates) as being those persons residing in Florida impacted by the Data Breach, including all who were sent a notice of the Data Breach (the "Florida Subclass").

89. Collectively, the Class and Florida Subclass are referred to as "the Classes."

90. Excluded from the Class are Defendants' officers and directors, and any entity in which Defendants have a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendants. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

91. Plaintiff reserves the right to amend or modify the Class or Subclass definitions as this case progresses.

92. **Numerosity**: Upon information and belief, the members of the Class are so

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

numerous that joinder of all of them is impracticable.

93. **Existence/Predominance of Common Questions of Fact and Law**: There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendants unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' PII;

b. 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;

c. Whether Defendants' data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendants' data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendants' owed a duty to Class Members to safeguard their PII;

f. Whether Defendants were subject to (and breached) the FTC Act or the Florida Deceptive And Unfair Trade Practices Act;

g. Whether Defendants breached their duties to Class Members to safeguard their PII;

h. Whether computer hackers obtained Class Members' PII in the Data Breach;

i. Whether Defendants knew or should have known that its data security systems and monitoring processes were deficient;

j. Whether Defendants' conduct was negligent;

k. Whether Defendants acts breaching an implied contract they formed with Plaintiff and the Class Members;

l. Whether Defendants were unjustly enriched to the detriment of Plaintiff and the Class;

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

m. Whether Defendants failed to provide notice of the Data Breach in a timely manner; and

n. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

94. **Typicality**: Plaintiff's claims are typical of those of other Class Members because Plaintiff's PII, like that of every other Class Member, were compromised in the Data Breach.

95. **Adequacy**: Plaintiff is an adequate representative for the Class because her interests do not conflict with the interests of the Class she seeks to represent. Plaintiff has retained counsel competent and highly experienced in complex class action litigation—including consumer fraud and automobile defect class action cases—and counsel intends to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and her experienced counsel.

96. **Superiority**: A class action is superior to all other available means of fair and efficient adjudication of the claims of Plaintiff and members of the Class. The injury suffered by each individual Class Member is relatively small in comparison to the burden and expense of individual prosecution of the complex and extensive litigation necessitated by Defendants' conduct. It would be virtually impossible for members of the Class individually to redress effectively the wrongs done to them by Defendants. Even if Class Members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties, and provides the benefits of single adjudication, an economy of scale, and comprehensive supervision by a single court. Upon information and belief, members of the Class can be readily identified and notified based upon, inter alia, the records (including databases, e-mails, dealership

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

records and files, etc.) Defendants maintain regarding their consumers.

97. Defendants have acted, and refuse to act, on grounds generally applicable to the Class, thereby making appropriate final equitable relief with respect to the Class as a whole.

CLAIMS FOR RELIEF

COUNT 1

NEGLIGENCE

(On Behalf of Plaintiff and the Nationwide Class)

98. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

99. Defendants owed a duty to Plaintiff and all other Class Members to exercise reasonable care in safeguarding and protecting their PII in its possession, custody, or control.

100. Defendants knew, or should have known, the risks of collecting and storing Plaintiff's and all other Class Members' PII and the importance of maintaining secure systems. Defendants knew, or should have known, of the vast uptick in data breaches in recent years. Defendants had a duty to protect the PII of Plaintiff and Class Members.

101. Given the nature of Defendants' business, the sensitivity and value of the PII they maintain, and the resources at its disposal, Defendants should have identified the vulnerabilities to its systems and prevented the Data Breach from occurring, which Defendants had a duty to prevent.

102. Defendants breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII entrusted to it—including Plaintiff's and Class Members' PII.

103. It was reasonably foreseeable to Defendants that their failure to exercise

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiff's and Class Members' PII to unauthorized individuals.

104. But for Defendants' negligent conduct or breach of the above-described duties owed to Plaintiff and Class Members, their PII would not have been compromised.

105. As a result of Defendants' above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and all other Class Members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, inter alia: (i) a substantially increased risk of identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well- established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face; and (vii) actual or attempted fraud.

COUNT II

NEGLIGENCE PER SE

(On Behalf of Plaintiff and the Nationwide Class)

106. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

107. Defendants' duties arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair…practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by a business, such as Defendants', of failing to employ reasonable measures to protect and secure PII.

108. Defendants violated Security Rules and Section 5 of the FTCA by failing to

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

use reasonable measures to protect Plaintiff's and all other Class Members' PII and not complying with applicable industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of PII it obtains and stores, and the foreseeable consequences of a data breach involving PII including, specifically, the substantial damages that would result to Plaintiff and the other Class Members.

109. Defendants' violations of Security Rules and Section 5 of the FTCA constitute negligence per se.

110. Plaintiff and Class Members are within the class of persons that Security Rules and Section 5 of the FTCA were intended to protect.

111. The harm occurring because of the Data Breach is the type of harm Security Rules and Section 5 of the FTCA were intended to guard against.

112. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiff's and Class Members' PII to unauthorized individuals.

113. The injury and harm that Plaintiff and the other Class Members suffered was the direct and proximate result of Defendants' violations of Security Rules and Section 5 of the FTCA. Plaintiff and Class Members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, inter alia: (i) a substantially increased risk of identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach; and (vi) actual or attempted fraud.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

COUNT III

BREACH OF FIDUCIARY DUTY

(On Behalf of Plaintiff and the Nationwide Class)

114. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

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

116. Defendants have a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of their relationship. They breached that duty by failing to properly protect the integrity of the system containing Plaintiff's and Class Members' PII, failing to safeguard the PII of Plaintiff and Class Members they collected.

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

COUNT IV

UNJUST ENRICHMENT

(On Behalf of Plaintiff and the Nationwide Class)

118. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein. This claim is pleaded in the alternative to the implied contract claim pursuant to Fed. R. Civ. P. 8(d).

119. Plaintiff and Class Members conferred a monetary benefit upon Defendants in the form of monies paid for production services or other services.

120. Defendants accepted or had knowledge of the benefits conferred upon it by Plaintiff and Class Members. Defendants also benefitted from the receipt of Plaintiff's and Class Members' PII.

121. As a result of Defendants' conduct, Plaintiff and Class Members suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures that Plaintiff and Class Members paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

122. Defendants should not be permitted to retain the money belonging to Plaintiff and Class Members because Defendants failed to adequately implement the data privacy and security procedures for itself that Plaintiff and Class Members paid for and that were otherwise mandated by federal, state, and local laws. and industry standards.

123. Defendants should be compelled to provide for the benefit of Plaintiff and Class Members all unlawful proceeds received by it because of the conduct and Data Breach alleged herein.

///

///

///

///

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

COUNT V

BREACH OF IMPLIED CONTRACT

(On Behalf of Plaintiff and the Nationwide Class)

124. Plaintiff realleges and incorporates by reference all allegations of the preceding factual allegations as though fully set forth herein.

125. Defendants required Plaintiff and Class Members to provide, or authorize the transfer of, their PII for Defendants to provide services. In exchange, Defendants entered implied contracts with Plaintiff and Class Members in which Defendants agreed to comply with their statutory and common law duties to protect Plaintiff's and Class Members' PII and to timely notify them in the event of a data breach.

126. Plaintiff and Class Members would not have provided their PII to Defendants had they known that Defendants would not safeguard their PII, as promised, or provide timely notice of a data breach.

127. Plaintiff and Class Members fully performed their obligations under their implied contracts with Defendants.

128. Defendants breached the implied contracts by failing to safeguard Plaintiff's and Class Members' PII and by failing to provide them with timely and accurate notice of the Data Breach.

129. The losses and damages Plaintiff and Class Members sustained (as described above) were the direct and proximate result of Defendants' breach of their implied contracts with Plaintiff and Class Members.

///

///

///

///

///

///

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

COUNT VI

VIOLATION OF FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT

Fla. Stat. §§ 501.201, *et seq.*

(On Behalf of Plaintiff and the Florida Subclass)

130. Plaintiff realleges and incorporates by reference every allegation contained elsewhere in this Complaint as if fully set forth herein.

131. Plaintiff and Florida Subclass Members are "consumers" as defined by Fla. Stat. § 501.203.

132. Defendants advertised, offered, or sold goods or services in Florida and engaged in trade or commerce directly or indirectly affecting the people of Florida.

133. Defendants engaged in unconscionable, unfair, and deceptive acts and practices in the conduct of trade and commerce, in violation of Fla. Stat. § 501.204(1), including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

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

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Florida's data security statute, F.S.A. § 501.171(2), which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of

Plaintiff's and Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Florida's data security statute, F.S.A. § 501.171(2);

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiff's and Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Florida's data security statute, F.S.A. § 501.171(2).

134. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

135. Had Defendants disclosed to Plaintiff and Subclass Members that its data systems were not secure and, thus, were vulnerable to attack, Defendant would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Defendants were trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff' and Subclass Members. Defendants accepted the responsibility of protecting the data but kept the inadequate state of their security controls secret from the public. Accordingly, Plaintiff and Subclass Members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

136. As a direct and proximate result of Defendants' unconscionable, unfair, and deceptive acts and practices, Plaintiff and Florida Subclass Members have suffered and

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

will continue to suffer injury, ascertainable losses of money or property, and monetary and non- monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Defendants' services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

137. Plaintiff and Florida Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages under Fla. Stat. § 501.211; declaratory and injunctive relief; reasonable attorneys' fees and costs, under Fla. Stat. § 501.2105(1); and any other relief that is just and proper.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Class, prays for judgment as follows:

a) For an Order certifying this action as a class action and appointing Plaintiff and her 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 equitable relief compelling Defendants to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII compromised during the Data Breach;

d) For an order requiring Defendants to pay for credit monitoring services for Plaintiff and the Class of a duration to be determined at trial;

e) For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

f) For an award of punitive damages, as allowable by law;

g) For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

h) Pre- and post-judgment interest on any amounts awarded; and

i) Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury on all claims so triable.

Dated: June 4, 2024

Respectfully submitted,
CLARKSON LAW FIRM, P.C.

By: */s/ Yana Hart*

Ryan J. Clarkson (SBN 257074)
rclarkson@clarksonlawfirm.com
Yana Hart (SBN 306499)
yhart@clarksonlawfirm.com
Tiara Avaness (SBN 343928)
tavaness@clarksonlawfirm.com
22525 Pacific Coast Highway
Malibu, CA 90265
Tel: (213) 788-4050
Fax: (213) 788-4070

NUSSBAUM LAW GROUP, P.C.
Linda P. Nussbaum*
lnussbaum@nussbaumpc.com
1133 Avenue of the Americas, 31st Floor
New York, NY 10036
Telephone: (917) 438-9189

CRIDEN & LOVE, P.A.
Michael E. Criden*
mcriden@cridenlove.com
Lindsey C. Grossman*
lgrossman@cridenlove.com
7301 SW 57th Court, Suite 515
South Miami, Florida 33143
Telephone: 305-357-9000
Fax: 305-357-9050

* *Pro Hac Vice Application Forthcoming*

Attorneys for Plaintiff and the Proposed Classes