Cristina Perez Hesano (#027023)
cperez@perezlawgroup.com
PEREZ LAW GROUP, PLLC
7508 N. 59th Avenue
Glendale, AZ 85301
Telephone: 602.730.7100
Fax: 623.235.6173

William B. Federman*
wbf@federmanlaw.com
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, OK 73120
Telephone: (405) 235-1560
Fax: (405) 239-2112

**Pro Hac Vice* application to be submitted

Counsel for Plaintiff and the Proposed Class

UNITED STATES DISTRICT COURT

DISTRICT OF ARIZONA

Daniel Davila, individually and on behalf of all similarly situated persons, Plaintiff, v. New Enchantment Group, LLC, Defendant.	Case No.: CLASS ACTION COMPLAINT JURY TRIAL DEMANDED

Plaintiff Daniel Davila, ("Plaintiff") individually and on behalf of all others similarly situated, brings this class action lawsuit against Defendant New Enchantment

Group, LLC ("Defendant" or "NEG"). The following allegations are based on Plaintiff's knowledge, investigation of counsel, facts of public record, and information and belief.

I. NATURE OF THE ACTION

1. Plaintiff seeks to hold NEG,—a limited liability company that develops and manages resorts, spas, and golf courses,—responsible for the injuries it inflicted on Plaintiff and approximately **5,568** similarly situated persons (the "Class" or "Class Members").[1] NEG was negligent in maintaining its data security and cybersecurity training and maintenance. This inadequacy and negligence led to a data breach ("Data Breach" or "Breach"). Because of NEG's negligence and inadequate cyber and data security, Plaintiff's and Class Members' highly sensitive and confidential personal information was exposed to cybercriminals.

2. The data that NEG exposed to cybercriminals was highly sensitive. The exposed data included (at least) personal identifying information ("PII") like Social Security Numbers, names, driver's license numbers, financial account numbers or credit/debit card numbers (in combination with security codes, access codes, passwords, or pins for the account).[2] The data exposed also included protected health information ("PHI") like health insurance information.[3]

[1] *See* https://www.mass.gov/doc/assigned-data-breach-number-29112-new-enchantment-group-llc/download.

[2] *Id.*; *see also* https://apps.web.maine.gov/online/aeviewer/ME/40/30046e47-1276-423e-99c3-0669e44e44ef.shtml.

[3] *See* https://ago.vermont.gov/sites/ago/files/2023-03/2023-02-28%20New%20Enchantment%20Group%20Data%20Breach%20Notice%20to%20Consumers.pdf.

3. NEG collected PII and PHI (collectively, the "Private Information") and then maintained that sensitive data in a negligent and/or reckless manner. As evidenced by the Data Breach, NEG negligently and inadequately maintained its network—rendering it easy prey for cybercriminals.

4. According to information and belief, the risk of the Data Breach was known to NEG. Thus, NEG was on notice that its inadequate data security created a heightened risk of exposure, compromise, and theft.

5. After the Data Breach, NEG failed to provide timely notice to the exposed Plaintiff and Class Members—thereby exacerbating their injuries. NEG's dilatory notice deprived Plaintiff and Class Members of the chance to take speedy measures to protect themselves and mitigate harm. Simply put, NEG impermissibly left Plaintiff and Class Members in the dark—thereby causing their injuries to fester and the damage to spread.

6. Even when NEG finally notified Plaintiff and Class Members of their exposure, NEG failed to adequately describe what information was compromised.

7. Today, the identities of Plaintiff and Class Members are in jeopardy—all due to NEG's negligence. Specifically, Plaintiff and Class Members now suffer from a present and continuing risk of fraud and identity theft. And now, Plaintiff and Class Members must constantly monitor their credit reports and financial accounts.

8. Armed with the sensitive Private Information stolen in the Data Breach, criminals can commit a litany of crimes. Specifically, criminals can now open new financial accounts in Class Members' names, take out loans using Class Members' identities, use Class Members' names to obtain medical services, use Class Members' health information to craft phishing and other hacking attacks based on Class Members'

individual health needs, use Class Members' identities to obtain government benefits, file fraudulent tax returns using Class Members' information, obtain driver's licenses in Class Members' names (but with another person's photograph), and give false information to police during an arrest.

9. Plaintiff and Class Members will likely suffer additional financial costs for purchasing necessary credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

10. Plaintiff and Class Members have suffered—and will continue to suffer—from the loss of the benefit of their bargain, unexpected out-of-pocket expenses, lost or diminished value of their Private Information, emotional distress, and the value of their time reasonably incurred to mitigate the fallout of the NEG's Data Breach.

11. Through this action, Plaintiff seeks to remedy these injuries on behalf of himself and all similarly situated individuals whose Private Information was exposed and compromised in the Data Breach.

12. Plaintiff seeks remedies including, but not limited to, compensatory damages, treble damages, punitive damages, reimbursement of out-of-pocket costs, and injunctive relief—including improvements to NEG's data security systems, future annual audits, and adequate credit monitoring services funded by NEG.

13. Plaintiff brings this action against NEG and asserts claims for: (1) negligence, (2) breach of implied contract, (3) unjust enrichment, and (4) violations of Arizona's Consumer Fraud Act.

PARTIES

14. Plaintiff **Daniel Davila** is a natural person and citizen of Arizona. He has no intention of moving to a different state in the immediate future. Plaintiff received a Notice of Data Breach Letter ("Notice Letter") from Defendant dated June 6, 2023, on or around June 8, 2023, notifying him that his name, Social Security number, and health insurance information were stolen in the Data Breach.[4]

15. Defendant **New Enchantment Group, LLC** is a Delaware limited liability company, registered as a foreign LLC in the State of Arizona, with its principal place of business at 16430 N. Scottsdale Rd., Suite 115, Scottsdale, Arizona, 85254.

JURISDICTION AND VENUE

16. This Court has original jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because this is a class action involving more than 100 putative class members and the amount in controversy exceeds $5,000,000, exclusive of interest and costs. And minimal diversity is established because, upon information and belief, many members of the Class are citizens of states different than Defendant's.

17. This Court has general personal jurisdiction over NEG because NEG's principal place of business and headquarters are in Scottsdale, Arizona. NEG regularly conducts substantial business in and from Arizona.

18. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1391(c)(2) because substantial events giving rise to the claims emanated from activities within this District, and NEG conducts substantial business in this District.

[4] *See* **Exhibit 1**.

FACTUAL ALLEGATIONS

NEG Collected and Stored the Private Information of Plaintiff and Class Members

19. Defendant NEG is a company that manages and develops resorts, spas, and golf courses.[5] In connection with the development and management of these properties, NEG receives certain information belonging to resort employees and other individuals.[6] This information includes the Private Information of Plaintiff and the Class, which is stored on NEG's computer systems, even when the person may no longer be employed by NEG.

20. Because of the highly sensitive and personal nature of the information Defendant acquires and stores, NEG knows or reasonably should have known that it stores Private Information and must comply with industry standards related to data security and all federal and state laws protecting employees' and other individuals' Private Information and provide adequate notice to employees' and other individuals' if their PII or PHI is disclosed without proper authorization.

21. When NEG collects this sensitive information, NEG assumes a duty of care to use reasonable measures to safeguard the Private Information from theft and misuse.

[5] *See* https://www.mass.gov/doc/assigned-data-breach-number-29112-new-enchantment-group-llc/download; https://apps.web.maine.gov/online/aeviewer/ME/40/30046e47-1276-423e-99c3-0669e44e44ef.shtml; https://ago.vermont.gov/sites/ago/files/2023-03/2023-02-28%20New%20Enchantment%20Group%20Data%20Breach%20Notice%20to%20Consumers.pdf.

[6] *Id.*

22. NEG acquired, collected, and stored Plaintiff's and Class Members' Private Information.

23. On information and belief, NEG acquired, *inter alia*, the following types of information: Social Security Numbers, names, driver's license numbers, financial account numbers or credit/debit card numbers (in combination with security codes, access codes, passwords, or pins for the account) and health insurance information.

24. By obtaining, collecting, and storing Plaintiff's and Class Members' Private Information, NEG assumed legal and equitable duties and knew, or should have known, that it was thereafter responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure.

25. Upon information and belief, Plaintiff and Class Members relied on NEG to keep their Private Information confidential and securely maintained, to use this information for business and employment purposes only, and to make only authorized disclosures of this information.

26. NEG could have prevented the Data Breach by properly securing and encrypting and/or more securely encrypting its servers generally, as well as Plaintiff's and Class Members' Private Information.

27. NEG's negligence in safeguarding Plaintiff's and Class Members' Private Information was exacerbated by repeated warnings and alerts directed to the increased need to protect and secure sensitive data, as evidenced by the trending data breach attacks in recent years.

28. Despite the prevalence of public announcements of data breaches and data security compromises, NEG failed to take appropriate steps to protect Plaintiff's and Class Members' Private Information from being compromised.

29. NEG failed to properly monitor and log the ingress and egress of network traffic for malware, such as ransomware.

30. NEG failed to properly monitor and log file access and modifications.

31. NEG failed to ensure file integrity.

32. NEG failed to properly train its employees as to cybersecurity awareness and best practices, specifically, how to avoid, detect, and report email phishing attacks.

33. NEG failed to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiff and Class Members.

34. NEG failed to timely and accurately disclose that Plaintiff's and Class Members' Private Information had been improperly acquired or accessed.

35. NEG knowingly disregarded standard information security principles, despite obvious risks, by allowing unmonitored and unrestricted access to unsecured Private Information.

36. NEG failed to provide adequate supervision and oversight of the Private Information with which it was and is entrusted, despite the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather Private Information of Plaintiff and Class Members, misuse the Private Information and potentially disclose it to others without consent.

37. Upon information and belief, failed to delete former employees' information after the employment was terminated.

38. According to information and belief, NEG failed to adequately train its employees to not store Private Information longer than absolutely necessary.

39. Upon information and belief, NEG failed to implement procedures so that Private Information was maintained no longer than absolutely necessary.

40. Upon information and belief, NEG failed to consistently enforce security policies aimed at protecting Plaintiff's and the Class Members' Private Information.

41. Upon information and belief, NEG failed to implement sufficient processes to quickly detect data breaches, security incidents, or intrusions.

42. Upon information and belief, NEG failed to encrypt Plaintiff's and Class Members' Private Information and monitor user behavior and activity to identify possible threats.

NEG's Data Breach

43. On October 4, 2022, NEG discovered unusual activity on its systems and determined that certain data had been encrypted by a third-party.[7] NEG discovered that cybercriminals had unrestricted access to its files and systems from October 3, 2022, to October 4, 2022.[8]

44. After an investigation, NEG admitted that "the unknown third party ***accessed and acquired*** certain documents from [its] systems during this period."[9] Based

[7] *Id.*

[8] *Id.*

[9] *Id.* (emphasis added).

on this admission, Plaintiff's and Class Members' Private Information was stolen during the Data Breach and is in the hands of cybercriminals.

45. On information and belief, cybercriminals were able to breach NEG's systems because NEG did not maintain reasonable security safeguards or protocols to protect Plaintiff's and the Class's Private Information, leaving it an unguarded target for theft and misuse. NEG admits as much in its Notice Letter sent to victims, admitting that after the fact: "we have taken steps to reduce the risk of this type of incident occurring in the future, including enhancing or technical security measures."[10]

46. Simply put, Defendant should have implemented those enhanced "technical security measures" years ago—thereby preventing the Data Breach and all of Plaintiff and Class Members' injuries.

47. While NEG claims to have become aware of the Data Breach as early as October 4, 2022, NEG delayed notifying victims of the Data Breach. NEG completed a review of the documents acquired during the Data Breach on December 9, 2022, but did not begin issuing Notice of Data Breach letters until in or around February 2023.[11] Shockingly, on April 5, 2023, NEG revealed ***additional documents*** were acquired by the cybercriminals during the Data Breach and sent out ***another*** batch of Notice of Data Breach letters on or around May 6, 2023.[12] NEG has no valid excuse for delaying notice

---

[10] *Id.*

[11] *Id.*

[12] *See* **Exhibit 1** (Plaintiff's Notice of Data Breach Letter).

to victims of the Data Breach or for failing to identify all of the individuals impacted by the Data Breach the first time it sent out Notice Letters.

48. Time is of the essence when highly sensitive Private Information is subject to unauthorized access and/or acquisition. The disclosed, accessed, and acquired Private Information of Plaintiff and Class Members is likely available on the Dark Web. Hackers can access and then offer for sale the unencrypted, unredacted Private Information to criminals. Plaintiff and Class Members are now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from the possible publication of their Private Information, especially their Social Security Numbers onto the Dark Web. Plaintiff and Class Members now face a lifetime risk of identity theft, which is heightened here by unauthorized access, theft, and/or disclosure of thousands of Social Security Numbers.

49. Following the Breach, and recognizing that each Class Member is now subject to the present and continuing risk of identity theft and fraud, NEG's Notice of Data Breach Letter encouraged Plaintiff and the Class to "take advantage" of the measly one (1) year of credit monitoring offered to Plaintiff and the Class. Such measures are insufficient to protect Plaintiff and Class Members from the lifetime risks each now face. As another element of damages, Plaintiff and Class Members seek a sum of money sufficient to provide to Plaintiff and Class Members identity theft protective services for their respective lifetimes.

50. Time is a compensable and valuable resource in the United States. According to the U.S. Bureau of Labor Statistics, 55.5% of U.S.-based workers are compensated on an hourly basis, while the other 44.5% are salaried.[13]

51. According to the U.S. Bureau of Labor Statistics' 2018 American Time Use Survey, American adults have only 36 to 40 hours of "leisure time" outside of work per week;[14] leisure time is defined as time not occupied with work or chores and is "the time equivalent of 'disposable income.'"[15] Usually, this time can be spent at the option and choice of the consumer, however, having been notified of the Data Breach, consumers now have to spend hours of their leisure time self-monitoring their accounts, communicating with financial institutions and government entities, and placing other prophylactic measures in place to attempt to protect themselves.

52. Plaintiff and Class Members are now deprived of the choice as to how to spend their valuable free hours and seek renumeration for the loss of valuable time as another element of damages.

---

[13] *Characteristics of minimum wage workers, 2020*, U.S. BUREAU OF LABOR STATISTICS https://www.bls.gov/opub/reports/minimum-wage/2020/home.htm#:~:text=In%202020%2C%2073.3%20million%20workers,wage%20of%20%247.25%20per%20hour; *Average Weekly Wage Data*, U.S. BUREAU OF LABOR STATISTICS, *Average Weekly Wage Data,* https://data.bls.gov/cew/apps/table_maker/v4/table_maker.htm%23type=1&year=2021&qtr=3&own=5&ind=10&supp=0 (last accessed Aug. 2, 2022) (finding that on average, private-sector workers make $1,253 per 40-hour work week.).

[14] Cory Stieg, *You're spending your free time wrong — here's what to do to be happier and more successful*, CNBC https://www.cnbc.com/2019/11/06/how-successful-people-spend-leisure-time-james-wallman.html (Nov. 6, 2019).

[15] *Id.*

53. Upon information and belief, the unauthorized third-party cybercriminals gained access to Plaintiff's and Class Members' Private Information with the intent of engaging in misuse of the Private Information and financial information, including marketing, and selling Plaintiff's and Class Members' Private Information.

54. NEG had and continues to have obligations created by reasonable industry standards, common law, state statutory law, and its own assurances and representations to keep Plaintiff's and Class Members' Private Information confidential and to protect such Private Information from unauthorized access.

55. NEG's Breach Notice letter omits the size and scope of the breach. NEG has demonstrated a pattern of providing inadequate notices and disclosures about the Data Breach (as evidenced by the two separate batches of Notice of Data Breach Letters).

56. Plaintiff and the Class Members remain, even today, are in the dark regarding what particular data was stolen, the particular ransomware used, and what steps are being taken, if any, to secure their Private Information going forward. Plaintiff and Class Members are left to speculate as to the full impact of the Data Breach and how exactly NEG intends to enhance its information security systems and monitoring capabilities so as to prevent further breaches.

57. Plaintiff's and Class Members' Private Information and financial information may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiff and/or Class Members. Either way, unauthorized individuals can now easily access the Private Information of Plaintiff and Class Members.

NEG Failed to Comply with FTC Guidelines

58. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making.[16] To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as NEG, should employ to protect against the unlawful exposure of Personal Information.

59. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[17] The guidelines explain that businesses should:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

60. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

61. The FTC recommends that companies not maintain Private Information 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

[16] *Start with Security: A Guide for Business*, FED. TRADE COMM'N (June 2015), https://bit.ly/3uSoYWF.
[17] *Protecting Personal Information: A Guide for Business*, FED. TRADE COMM'N (Oct. 2016), https://bit.ly/3u9mzre.

security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[18]

62. 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.

63. NEG's failure to employ reasonable and appropriate measures to protect against unauthorized access to the Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

NEG Failed to Follow Industry Standards

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

65. Such frameworks are the existing and applicable industry standards. And NEG failed to comply with these accepted standards—thus opening the door to criminals and the Data Breach.

[18] *See Start with Security*, *supra* note 15.

The Experiences and Injuries of Plaintiff & the Class

66. Plaintiff and Class Members are employees and/or customers of NEG. As a prerequisite of employment and/or using the resorts, spas, and golf courses NEG manages and develops, Plaintiff and the Class were required to disclose their Private Information.

67. NEG began notifying victims of the Data Breach on or around February 23, 2023 — ***approximately 4 months after discovering the Breach***. NEG failed to explain why it took approximately 4 months to notify victims. To make matters worse, on April 5, 2023, NEG revealed ***additional documents*** were acquired by the cybercriminals during the Data Breach and sent out ***another*** batch of Notice of Data Breach Letters – ***approximately 7 months after discovering the Breach***.[19] NEG has no valid excuse for delaying notice to victims of the Data Breach. NEG does not state why it did not discover all of the individuals impacted the first time it reviewed the documents either.

68. When NEG finally announced the Data Breach, it deliberately underplayed the Breach's severity and obfuscated the nature of the Breach.

69. Because of the Data Breach, NEG inflicted injuries upon Plaintiff and Class Members. And yet, NEG has done barely anything to provide Plaintiff and the Class Members with relief for the damages they suffered and will suffer.

70. All the Plaintiff were injured when Defendant exposed their Private Information. Specifically, Defendant injured Plaintiff by compromising, *inter alia*, health insurance information, Social Security Numbers, names, driver's license numbers, and

[19] *See* **Exhibit 1** (Plaintiff's Notice of Data Breach Letter).

financial account numbers or credit/debit card numbers (in combination with security codes, access codes, passwords, or pins for the account).

71. Plaintiff entrusted their Private Information to NEG. By accepting Plaintiff's and the Class's PII it undertook the obligation and duty to protect and maintain the confidentiality of Private Information entrusted to it. Thus, Plaintiff had the reasonable expectation and understanding that NEG would take—*at minimum*—industry standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify them of any data security incidents. After all, Plaintiff would not have entrusted his Private Information to NEG had he known that NEG would not take reasonable steps to safeguard his information.

72. Plaintiff suffered actual injury from having his Private Information compromised because of the Data Breach including, but not limited to (a) damage to and diminution in the value of his Private Information—a form of property that NEG obtained from Plaintiff; (b) violation of his privacy rights; (c) the theft of his Private Information; (d) lost time spent investigating and addressing the effects of the Data Breach; (e) out of pocket expenses for credit monitoring; and/or (f) present and continuing injury arising from the present and continuing risk of identity theft and fraud.

73. As a result of the Data Breach, Plaintiff also suffered emotional distress because of the release of his Private Information—which he believed would be protected from unauthorized access and disclosure. Now, Plaintiff suffers from anxiety about unauthorized parties viewing, selling, and/or using his Private Information for nefarious purposes like identity theft and fraud.

74. And Plaintiff also suffered anxiety about unauthorized parties viewing, using, and/or publishing his information.

75. Because of the Data Breach, Plaintiff has spent—and will continue to spend—considerable time and money to try to mitigate and address harms caused by the Data Breach.

Plaintiff's Experience

76. Plaintiff Davila was an employee of NEG and provided his Private Information to NEG to receive employment and/or elective benefits.

77. Plaintiff entrusted his Private Information to NEG with the reasonable expectation and understanding that NEG would take at a minimum, industry standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify him of any data security incidents related to him. Plaintiff would not have used NEG's services and/or accepted employment had he known that NEG would not take reasonable steps to safeguard his Private Information.

78. In or around June 8, 2023, Plaintiff received a Notice of Data Breach Letter from NEG, notifying him that his name, Social Security Number, and health insurance information had been improperly accessed and obtained by unauthorized cybercriminals.

79. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach after receiving the Notice of Data Breach Letter, including but not limited to researching the Data Breach and reviewing credit card and financial account statements.

80. Plaintiff has spent a few hours and will continue to spend valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation.

81. Plaintiff suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his Private Information, a form of property that NEG obtained from Plaintiff; (b) violation of his privacy rights; (b) the theft of his Private Information; and (d) imminent and impending injury arising from the increased risk of identity theft and fraud.

82. As a result of the Data Breach, Plaintiff has also suffered emotional distress as a result of the release of his Private Information, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his Private Information for purposes of identity theft and fraud. Plaintiff is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach. Plaintiff also has suffered anxiety about unauthorized parties viewing, using, and/or publishing his information.

83. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff will continue to be at present, imminent, and continued increased risk of identity theft and fraud for years to come.

Plaintiff and the Proposed Class Face Significant Risk of Present and Continuing Identity Theft

84. Plaintiff and Class Members suffered injury from the misuse of their Private Information that can be directly traced to NEG.

85. The ramifications of NEG's failure to keep Plaintiff's and the Class's Private Information secure are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security Number, driver's license number, date of birth, and/or other information, without permission, to commit fraud or other crimes.

86. According to experts, one out of four data breach notification recipients become a victim of identity fraud.[20]

87. As a result of NEG's failures to prevent—and to timely detect—the Data Breach, Plaintiff and Class Members suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at a present risk of suffering:

a. The loss of the opportunity to control how their Private Information is used;

b. The diminution in value of their Private Information;

c. The compromise and continuing publication of their Private Information;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

[20] *More Than 12 Million Identity Fraud Victims in 2012 According to Latest Javelin Strategy & Research Report*, BUSINESSWIRE (Feb. 20, 2013) https://threatpost.com/study-shows-one-four-who-receive-data-breach-letter-become-fraud-victims-022013/77549/.

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen Private Information; and

h. The continued risk to their Private Information, which remains in the possession of NEG and is subject to further breaches so long as NEG fails to undertake the appropriate measures to protect the Private Information in its possession.

88. Stolen Private Information is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen Private Information can be worth up to $1,000.00 depending on the type of information obtained.[21]

89. The value of Plaintiff's and the proposed Class's Private Information on the black market is considerable. Stolen Private Information trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

[21] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN (Dec. 6, 2017) https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.

90. It can take victims years to spot or identify Private Information theft, giving criminals plenty of time to milk that information for cash.

91. One such example of criminals using Private Information for profit is the development of "Fullz" packages.[22]

92. Cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

93. The development of "Fullz" packages means that stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiff's and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam

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

telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and other members of the proposed Class's stolen Private Information is being misused, and that such misuse is fairly traceable to the Data Breach.

94. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.

95. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good." NEG did not rapidly report to Plaintiff and the Class that their Private Information had been stolen.

96. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

97. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims have to spend a considerable time repairing the damage caused by the theft of their Private Information. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

98. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen Private Information. To protect

themselves, Plaintiff and the Class will need to remain vigilant against unauthorized data use for years or even decades to come.

99. The Federal Trade Commission ("FTC") has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency."[23]

100. The FTC has also issued numerous guidelines for businesses that highlight the importance of reasonable data security practices. The FTC has noted the need to factor data security into all business decision-making.[24] According to the FTC, data security requires: (1) encrypting information stored on computer networks; (2) retaining payment card information only as long as necessary; (3) properly disposing of personal information that is no longer needed; (4) limiting administrative access to business systems; (5) using industry-tested and accepted methods for securing data; (6) monitoring activity on networks to uncover unapproved activity; (7) verifying that privacy and security features function properly; (8) testing for common vulnerabilities; and (9) updating and patching third-party software.[25]

---

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

[24] *Start With Security, A Guide for Business*, FED. TRADE COMMISSION, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[25] *Id.*

101. According to the FTC, unauthorized Private Information disclosures are extremely damaging to consumers' finances, credit history and reputation, and can take time, money, and patience to resolve the fallout.[26] The FTC treats 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(a) of the FTC Act (the "FTCA").

102. To that end, the FTC has issued orders against businesses that failed to employ reasonable measures to secure sensitive payment card data. *See In the matter of Lookout Services, Inc.*, No. C-4326, ¶ 7 (June 15, 2011) ("[Defendant] allowed users to bypass authentication procedures" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks, such as employing an intrusion detection system and monitoring system logs."); *In the matter of DSW, Inc.*, No. C-4157, ¶ 7 (Mar. 7, 2006) ("[Defendant] failed to employ sufficient measures to detect unauthorized access."); *In the matter of The TJX Cos., Inc.*, No. C-4227 (Jul. 29, 2008) ("[R]espondent stored . . . personal information obtained to verify checks and process unreceipted returns in clear text on its in-store and corporate networks[,]" "did not require network administrators . . . to use different passwords to access different programs, computers, and networks[,]" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks . . ."); *In the matter of Dave & Buster's Inc.*, No. C-4291 (May 20, 2010) ("[Defendant] failed to monitor and filter outbound

[26] *See Taking Charge, What to Do If Your Identity is Stolen*, FED. TRADE COMMISSION, at 3 (2012), https://www.ojp.gov/ncjrs/virtual-library/abstracts/taking-charge-what-do-if-your-identity -stolen.

traffic from its networks to identify and block export of sensitive personal information without authorization" and "failed to use readily available security measures to limit access between instore networks . . ."). These orders, which all preceded the Data Breach, further clarify the measures businesses must take to meet their data security obligations. NEG thus knew or should have known that its data security protocols were inadequate and were likely to result in the unauthorized access to and/or theft of Private Information.

103. Over the past several years, data breaches have become alarmingly commonplace. In 2016, the number of data breaches in the U.S. exceeded 1,000, a 40% increase from 2015.[27] The next year, that number increased by nearly 45%.[28]

104. Charged with handling highly sensitive Personal Information including health insurance information, Social Security numbers, and financial information, NEG knew or should have known the importance of safeguarding the Personal Information that was entrusted to it. NEG also knew or should have known of the foreseeable consequences if its data security systems were breached. This includes the significant costs that would be imposed on NEG's employees and customers because of a breach. NEG nevertheless failed to take adequate cybersecurity measures to prevent the Data Breach from occurring.

105. NEG disclosed the Private Information of Plaintiff and members of the proposed Class for criminals to use in the conduct of criminal activity. Specifically, NEG opened, disclosed, and exposed the Private Information of Plaintiff and members of the

[27] *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout*, IDENTITY THEFT RESOURCE CENTER (Jan. 19, 2017), https://bit.ly/30Gew91 [hereinafter "*Data Breaches Increase 40 Percent in 2016*"].

[28] *Data Breaches Up Nearly 45 Percent According to Annual Review by Identity Thegt Resource Center® and CyberScout®*, IDENTITY THEFT RESOURCE CENTER (Jan. 22, 2018), https://bit.ly/3jdGcYR [hereinafter "*Data Breaches Up Nearly 45 Percent*"].

proposed Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen Private Information.

106. NEG's use of outdated and insecure computer systems and software that are easy to hack, and its failure to maintain adequate security measures and an up-to-date technology security strategy, demonstrates a willful and conscious disregard for privacy, and has exposed the Private Information of Plaintiff and potentially thousands of members of the proposed Class to unscrupulous operators, con artists, and outright criminals. NEG certainly knew, or should have known, that entities harboring Private Information are particularly vulnerable to cyberattacks and that, as a result, it must take steps to protect the trove of Private Information it holds.

107. Yet, on information and belief, NEG failed to implement even the most basic levels of cybersecurity.

108. NEG's failure to properly notify Plaintiff and members of the proposed Class of the Data Breach then exacerbated Plaintiff's and members of the proposed Class's injury by depriving them of the earliest ability to take appropriate measures to protect their Private Information and take other necessary steps to mitigate the harm caused by the Data Breach.

CLASS ACTION ALLEGATIONS

109. Plaintiff brings this action on behalf of themselves and on behalf of all other persons similarly situated ("the Class") under Fed. R. Civ. P. 23(b)(2), 23(b)(3), and 23(c)(4).

110. Plaintiff proposes the following Class definitions, subject to amendment as appropriate:

> **All persons residing in the United States that NEG identified as persons impacted by the Data Breach—including all persons that Defendant sent a Notice of Data Breach Letter to (the "Class").**

111. The Classes defined above are readily ascertainable from information in NEG's possession. Thus, such identification of Class Members will be reliable and administratively feasible.

112. Excluded from the Classes are: (1) any judge or magistrate presiding over this action and members of their families; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, affiliated entities, and any entity in which Defendant or its parent has a controlling interest; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and Defendant's counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

113. Plaintiff reserves the right to amend or modify the Class definitions—including potential Subclasses—as this case progresses.

114. Plaintiff satisfies the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

115. **Numerosity**. The Class Members are numerous such that joinder is impracticable. While the exact number of Class Members is unknown to Plaintiff at this

time, based on information and belief, the Classes consists of over **5,000** individuals whose Private Information were compromised by NEG's Data Breach.

116. **Commonality**. There are many questions of law and fact common to the Classes. And these common questions predominate over any individualized questions of individual Class Members. These common questions of law and fact include, without limitation:

a. If NEG unlawfully maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;

b. If NEG 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. If NEG's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations including;

d. If NEG's data security systems prior to and during the Data Breach were consistent with industry standards;

e. If NEG owed a duty to Class Members to safeguard their Private Information;

f. If NEG breached its duty to Class Members to safeguard their Private Information;

g. If NEG knew or should have known that its data security systems and monitoring processes were deficient;

h. If NEG should have discovered the Data Breach earlier;

i. If NEG took reasonable measures to determine the extent of the Data Breach after it was discovered;

j. If NEG's delay in informing Plaintiff and Class Members of the Data Breach was unreasonable;

k. If NEG's method of informing Plaintiff and Class Members of the Data Breach was unreasonable;

l. If NEG's conduct was negligent;

m. If Plaintiff and Class Members were injured as a proximate cause or result of the Data Breach;

n. If Plaintiff and Class Members suffered legally cognizable damages as a result of NEG's misconduct;

o. If NEG breached implied contracts with Plaintiff and Class Members;

p. If NEG violated the consumer protection statutes invoked herein;

q. If NEG was unjustly enriched by unlawfully retaining a benefit conferred upon it by Plaintiff and Class Members;

r. If NEG failed to provide notice of the Data Breach in a timely manner, and;

s. If Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

117. **Typicality**. Plaintiff's claims are typical of those of other Class Members because Plaintiff's information, like that of every other Class Member, was compromised in the Data Breach. Moreover, all Plaintiff and Class Members were subjected to NEG's uniformly illegal and impermissible conduct.

118. **Adequacy of Representation**. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Classes. Plaintiff's Counsel are competent and experienced in litigating complex class actions. Plaintiff has no interests that conflict with, or are antagonistic to, those of the Classes.

119. **Predominance**. NEG has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff and Class Members' data was stored on the same computer system and unlawfully exposed in the same way. The common issues arising from NEG's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

120. **Superiority**. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for NEG. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources, the parties' resources, and protects the rights of each Class Member.

121. The litigation of the claims brought herein is manageable. NEG's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of

Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

122. Adequate notice can be given to Class Members directly using information maintained in NEG's records.

123. 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 those set forth above.

124. NEG has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiff and the Class)

125. Plaintiff re-alleges and incorporates by reference all other paragraphs in the Complaint as if fully set forth herein.

126. NEG required Plaintiff and Class Members, to provide their Private Information to receive employment, elective benefits, and/or services.

127. By collecting and storing this data in its computer system and network for its own commercial gain, NEG owed a duty of care to use reasonable means to secure and safeguard its computer system—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. NEG's duty included a responsibility to implement processes so it could detect a breach

of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

128. The risk that unauthorized persons would attempt to gain access to the Private Information and misuse it was foreseeable. Given that NEG holds vast amounts of Private Information, it was inevitable that unauthorized individuals would at some point try to access NEG's databases of Private Information.

129. After all, Private Information is highly valuable, and NEG knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the Private Information of Plaintiff and Class Members. Thus, NEG knew, or should have known, the importance of exercising reasonable care in handling the Private Information entrusted to it.

130. NEG owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

131. NEG's duty of care to use reasonable security measures arose because of the special relationship that existed between NEG, its employees, and its customers, which is recognized by laws and regulations including the FTC Act, as well as common law. NEG was in a superior position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

132. Under the Federal Trade Commission Act, NEG had a duty to employ reasonable security measures. Specifically, this statute prohibits "unfair . . . practices in or

affecting commerce," including (as interpreted and enforced by the FTC) the unfair practice of failing to use reasonable measures to protect confidential data.[29]

133. Moreover, Plaintiff and Class Members' injuries are precisely the type of injuries that the FTC Act guards against. After all, the FTC has pursued numerous enforcement actions against businesses that—because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices—caused the very same injuries that Defendant inflicted upon Plaintiff and Class Members.

134. Under the Arizona Data Breach Notification Act, NEG has a duty to promptly notify affected persons so they can take action to protect themselves if "the investigation [of a potential data breach] results in a determination that there has been a security system breach, the person that owns or licenses the computerized data, within forty-five days after the determination, shall . . . [n]otify the individuals affected."[30]

135. Moreover, Plaintiff and Class Members' injuries are precisely the type of injuries that the Arizona Data Breach Notification Act guards against.

136. NEG's duty to use reasonable care in protecting confidential data arose not only because of the statutes and regulations described above, but also because NEG is bound by industry standards to protect confidential Private Information.

137. NEG owed Plaintiff and members of the Class a duty to notify them within a reasonable time frame of any breach to their Private Information. Defendant also owed a duty to timely and accurately disclose to Plaintiff and members of the Class the scope, nature, and occurrence of the Data Breach. This duty is necessary for Plaintiff and Class

[29] 15 U.S.C. § 45.
[30] A.R.S §§ 18-551, 18-552.

Members to take appropriate measures to protect their Private Information, to be vigilant in the face of an increased risk of harm, and to take other necessary steps in an effort to mitigate the fallout of NEG's Data Breach.

138. NEG owed these duties to Plaintiff and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom NEG knew or should have known would suffer injury-in-fact from its inadequate security protocols. After all, NEG actively sought and obtained the Private Information of Plaintiff and Class Members.

139. NEG breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. And but for NEG's negligence, Plaintiff and Class Members would not have been injured. The specific negligent acts and omissions committed by NEG include, but are not limited to:

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

b. Failing to comply with—and thus violating—FTC Act and its regulations;

c. Failing to comply with—and thus violating—the Arizona Data Breach Notification Act and its regulations;

d. Failing to adequately monitor the security of its networks and systems;

e. Failing to ensure that its email system had plans in place to maintain reasonable data security safeguards;

f. Failing to have in place mitigation policies and procedures;

g. Allowing unauthorized access to Class Members' Private Information;

h. Failing to detect in a timely manner that Class Members' Private Information had been compromised; and

i. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

140. It was foreseeable that NEG's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Furthermore, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

141. Simply put, NEG's negligence actually and proximately caused Plaintiff and Class Members' actual, tangible, injuries-in-fact, and damages. These injuries include, but are not limited to, the theft of their Private Information by criminals, improper disclosure of their Private Information, lost value of their Private Information, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by NEG's negligence. Moreover, injuries-in-fact and damages are ongoing, imminent, and immediate.

142. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered because of the Data Breach.

143. Plaintiff and Class Members are also entitled to injunctive relief requiring NEG to, *e.g.,* (1) strengthen its data security systems and monitoring procedures; (2)

submit to future annual audits of those systems and monitoring procedures; and (3) to provide adequate credit monitoring to all Class Members.

SECOND CAUSE OF ACTION
Breach of Implied Contract
(On behalf of the Plaintiff and the Class)

144. Plaintiff re-alleges and incorporates by reference all other paragraphs in the Complaint as if fully set forth herein.

145. Plaintiff and the Class Members entered into implied contracts with Defendant under which Defendant agreed to safeguard and protect their Private Information and to timely and accurately notify Plaintiff and Class Members that their information had been breached and compromised.

146. Plaintiff and the Class were required to, and delivered, their Private Information to Defendant as part of the process of obtaining services, employment, and/or elective benefits.

147. Plaintiff and Class Members conferred a monetary benefit on Defendant in that Defendant derived revenue from their labor, a precondition of which required Plaintiffs and Class members to entrust their Private Information to Defendant. Without the labor and Private Information provided by Plaintiffs and Class members, Defendant could not derive revenue from its regular business activities. A portion of the revenue derived from the labor and Private Information of Plaintiffs and Class members was to be used to provide a reasonable level of data security and practices, and the amount of revenue to be allocated to data security is known to Defendant.

148. Alternatively, Plaintiff and Class Members paid money to Defendant in exchange for services.

149. Defendant accepted possession of Plaintiff's and Class Members' Private Information for the purpose of providing services, employment, and/or elective benefits.

150. The implied promise of confidentiality includes consideration beyond those pre-existing general duties owed under state and federal regulations. The additional consideration included implied promises to take adequate steps to comply with specific industry data security standards and FTC guidelines on data security.

151. The implied promises include but are not limited to: (1) taking steps to ensure that any agents who are granted access to Private Information also protect the confidentiality of that data; (2) taking steps to ensure that the information that is placed in the control of its agents is restricted and limited to achieve an authorized purpose; (3) restricting access to qualified and trained agents; (4) designing and implementing appropriate retention policies to protect the information against criminal data breaches; (5) applying or requiring proper encryption; (6) multifactor authentication for access; and (7) other steps to protect against foreseeable data breaches.

152. Based on the implicit understanding, Plaintiff and Class Members accepted NEG's offers and provided NEG with their Private Information.

153. Plaintiff and Class Members would not have permitted their Private Information to be collected and stored by NEG had they known that NEG would not safeguard their Private Information, as promised, or provide timely notice of a data breach.

154. Plaintiff and Class Members fully performed their obligations under their implied contracts with NEG.

155. NEG breached the implied contracts by failing to safeguard Plaintiff's and Class Members' Private Information and by failing to provide them with timely and accurate notice of the Data Breach.

156. The losses and damages Plaintiff and Class Members sustained (as described above) were the direct and proximate result of NEG's breach of its implied contracts with Plaintiff and Class members.

THIRD CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

157. Plaintiff re-alleges and incorporates by reference all other paragraphs in the Complaint as if fully set forth herein.

158. This cause of action is plead in alternative to the breach of implied contract theory.

159. Plaintiff and Class Members conferred a benefit on NEG, by either paying money to NEG for services or providing NEG with their labor for employment that allowed NEG to receive revenue and profits. A portion of which was intended to have been used by NEG for data security measures to secure Plaintiff and Class Members' Private Information. Plaintiff and Class Members further conferred a benefit on NEG by entrusting their Private Information to it and from which NEG derived profits.

160. NEG enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff and Class Members' Private Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, NEG chose to avoid its data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class

Members, on the other hand, suffered as a direct and proximate result of NEG's failure to provide adequate security.

161. Under the principles of equity and good conscience, NEG should not be permitted to retain the money belonging to Plaintiff and Class Members, because NEG failed to implement appropriate data management and security measures that are mandated by industry standards.

162. NEG acquired the monetary benefit, PII, and PHI through inequitable means in that it failed to disclose the inadequate security practices previously alleged and failed to maintain adequate data security.

163. If Plaintiff and Class Members knew that NEG had not secured their Private Information, they would not have agreed to give their money—or disclose their data—to NEG.

164. Plaintiff and Class Members have no adequate remedy at law.

165. As a direct and proximate result of NEG's conduct, Plaintiff and Class Members have suffered—and will continue to suffer—a host of injuries, including but not limited to: (1) actual identity theft; (2) the loss of the opportunity to determine how their Private Information is used; (3) the compromise, publication, and/or theft of their Private Information; (4) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (5) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (6) the continued risk to their Private Information, which

remain in NEG's possession and are subject to further unauthorized disclosures so long as NEG fails to undertake appropriate and adequate measures to protect the Private Information in its possession; and (7) future expenditures of time, effort, and money that will be spent trying to prevent, detect, contest, and repair the impact of NEG's Data Breach.

166. As a direct and proximate result of NEG's conduct, Plaintiff and Class Members suffered—and will continue to suffer—other forms of injury and/or harm.

167. NEG should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that it unjustly received from Plaintiff and Class Members. Alternatively, NEG should be compelled to refund the amounts that Plaintiff and Class Members overpaid for NEG's services.

FOURTH CAUSE OF ACTION
Violations of the Arizona Consumer Fraud Act,
A.R.S. §§ 44-1521, *et seq.*
(On Behalf of Plaintiff and the Class)

168. Plaintiff re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

169. NEG is a "person" as defined by A.R.S. §44-1521(6).

170. NEG sold Plaintiff and Class Members "merchandise" as defined by A.R.S. § 44-1521, in the form of services in connection with the properties NEG managed.

171. Section 44-1522 of the Arizona Consumer Fraud Act provides:

> The act, use or employment by any person of any deception, deceptive or unfair act or practice, fraud, false pretense, false promise, misrepresentation, or concealment, suppression or omission of any material fact with intent that others rely on such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise whether or not any person has in fact been misled, deceived or damaged thereby.

A.R.S. § 44-1522(A).

172. NEG used deception, used a deceptive act or practice, and fraudulently omitted and concealed material facts in connection with the sale or advertisement of that merchandise in violation of A.R.S. § 44-1522(A).

173. NEG omitted and concealed material facts, which it knew about and had the duty to disclose—namely, NEG's inadequate privacy and security protections for Plaintiff's and Class Members' Private Information. This omission was designed to mislead consumers.

174. NEG omitted and concealed those material facts even though in equity and good conscience those facts should have been disclosed and did so with the intent that others would rely on the omission, suppression, and concealment.

175. Upon information and belief, NEG intentionally omitted and concealed material facts—like NEG's inadequate cyber and data privacy and security protections—with the intention that consumers rely on those omissions.

176. The concealed facts are material in that they are logically related to the transactions at issue and rationally significant to the parties in view of the nature and circumstances of those transactions.

177. Plaintiff and Class Members were ignorant of the truth and relied on the concealed facts in providing Private Information to NEG and incurred damages as a consequent and proximate result.

178. But for NEG's omissions, the damage to Plaintiff and Class Members would not have occurred.

179. Plaintiff do not allege any claims based on any affirmative misrepresentations by NEG. Rather, Plaintiff allege that NEG omitted, failed to disclose, and concealed material facts and information as alleged herein—despite its duty to disclose such facts and information.

180. NEG knew or should have known that its computer system and data security practices were inadequate to safeguard Plaintiff's and Class Members' Private Information, and that the risk of a data breach or theft was highly likely. NEG's actions in engaging in these deceptive acts and practices were intentional, knowing, willful, wanton, and reckless with respect to the rights of Plaintiff and Class Members.

181. Specifically, NEG failed to comply with the standards outlined by the FTC Act. NEG was or should have been aware of these standards. NEG's data security systems did not follow the FTC's guidelines. And thus, NEG's systems operated below the minimum standards required.

182. Plaintiff and Class Members were ignorant of the truth and relied on the concealed facts in providing their Private Information and incurred damages as a consequent and proximate result.

183. Plaintiff and Class Members seek all available relief under A.R.S. §§ 44-1521, *et seq.*, including, but not limited to, compensatory damages, punitive damages, injunctive relief, and attorneys' fees and costs.

PRAYER FOR RELIEF

WHEREFORE Plaintiff, on behalf of themselves and all others similarly situated, request the following relief:

A. An Order certifying this action as a class action and appointing Plaintiff as Class representative and the undersigned as Class counsel;

B. A mandatory injunction directing NEG to adequately safeguard the Private Information of Plaintiff and the Class hereinafter by implementing improved security procedures and measures, including but not limited to an Order:

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

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

iii. requiring NEG to delete and purge the Private Information of Plaintiff and Class Members unless NEG 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 NEG to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiff's and Class Members' Private Information;

v. requiring NEG to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests, and audits on NEG's systems on a periodic basis;

vi. prohibiting NEG from maintaining Plaintiff's and Class Members' Private Information on a cloud-based database;

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

viii. requiring NEG to conduct regular database scanning and securing checks;

ix. requiring NEG to monitor ingress and egress of all network traffic;

x. requiring NEG 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 Private Information, as well as protecting the Private Information of Plaintiff and Class Members;

xi. requiring NEG 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 NEG's policies, programs, and systems for protecting personal identifying information;

xii. requiring NEG to implement, maintain, review, and revise as necessary a threat management program to appropriately monitor NEG's networks for internal and external threats, and assess whether monitoring tools are properly configured, tested, and updated;

xiii. requiring NEG to meaningfully educate all Class Members about the threats that they face because of the loss of its confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves; and

xiv. requiring NEG to provide adequate credit monitoring to all Class Members.

C. A mandatory injunction requiring that NEG provide notice to each member of the Class relating to the full nature and extent of the Data Breach and the disclosure of Private Information to unauthorized persons;

D. Enjoining NEG from further deceptive practices and making untrue statements about the Data Breach and the stolen Private Information;

E. An award of damages, including actual, nominal, consequential damages, and punitive, as allowed by law in an amount to be determined;

F. An award of attorneys' fees, costs, and litigation expenses, as allowed by law;

G. An award of pre- and post-judgment interest, costs, attorneys' fees, expenses, and interest as permitted by law;

H. Granting the Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial;

I. For all other Orders, findings, and determinations identified and sought in this Complaint; and

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

JURY TRIAL DEMANDED

Under Federal Rule of Civil Procedure 38(b), Plaintiff demands a trial by jury for any and all issues in this action so triable as of right.

DATED: June 14, 2023

Respectfully Submitted,

/s/ Cristina Perez Hesano

Cristina Perez Hesano (#027023)
cperez@perezlawgroup.com
PEREZ LAW GROUP, PLLC
7508 N. 59th Avenue
Glendale, AZ 85301
Telephone: 602.730.7100
Fax: 623.235.6173

William B. Federman*
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, OK 73120
Telephone: (405) 235-1560
Email: wbf@federmanlaw.com

**Pro Hac Vice application to be submitted*

Counsel for Plaintiff and the Proposed Class

New Enchantment Group, LLC
Mail Handling Services
777 E Park Dr
Harrisburg, PA 17111

ENCHANTMENT GROUP

Daniel Davila J-269
[redacted]

June 6, 2023

Dear Daniel Davila:

RE: NOTICE OF DATA BREACH

New Enchantment Group, LLC ("NEG") values and respects the privacy of your information, which is why we are writing to advise you of an incident at NEG that involved some of your personal information. This letter explains the incident, the steps we have taken in response, and additional information on steps you may take to help protect your information.

What Happened? On October 4, 2022, we discovered unusual activity on NEG's computer network and determined that certain data had been encrypted by a third party. Upon identifying the issue, we promptly began an internal investigation, notified law enforcement, restored our data from backups, and secured our systems. We also engaged a forensic security firm to assist with our investigation. The forensic investigation determined that an unknown, unauthorized third party accessed NEG's computer systems from October 3, 2022 until October 4, 2022. The investigation determined that the third party acquired certain documents from our systems during this period. We completed a review of those documents on December 9, 2022 and did not identify any of your personal information in the documents. On April 5, 2023, we learned that the third party acquired additional documents from our systems during the incident.

What Information Was Involved? We reviewed the contents of the documents to determine if they contained any personal information. On May 4, 2023, we completed our review and determined that the acquired documents contained personal information that included your name, together with your Social Security number and health insurance information.

What We Are Doing. In addition to the actions described above, we have taken steps to reduce the risk of this type of incident occurring in the future, including enhancing our technical security measures. We are offering a complimentary one-year membership of Experian IdentityWorks℠ Credit 3B. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on prompt identification and resolution of identity theft. IdentityWorks Credit 3B is completely free to you, and enrolling in this program will not hurt your credit score. **For more information on identity theft prevention and IdentityWorks Credit 3B, including instructions on how to activate your complimentary one-year membership, please see the additional information provided in this letter.**

What You Can Do. We encourage you to take advantage of the complimentary credit monitoring included in this letter. You can also find more information on steps to protect yourself against identity theft or fraud in the enclosed *Additional Important Information* sheet.

For More Information. We value the trust you place in us to protect your privacy, take our responsibility to safeguard your personal information seriously, and apologize for any inconvenience this incident might cause. For further information and assistance, please call 800-511-4722 from 6 a.m. – 3 p.m. Mountain Standard Time, Monday through Friday.

Sincerely,

New Enchantment Group, LLC

ACTIVATING YOUR COMPLIMENTARY CREDIT MONITORING

To help protect your identity, we are offering a **complimentary** one-year membership of Experian IdentityWorks℠ Credit 3B. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: **8/31/2023** (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website to enroll: https://www.experianidworks.com/3bcredit**
3. PROVIDE the **Activation Code:** [redacted]

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-288-8057. Be prepared to provide engagement number [redacted] as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Activate your membership today at https://www.experianidworks.com/3bcredit
or call 877-288-8057 to register with the activation code above.

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-288-8057.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Additional Important Information

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Credit Reports: You may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies by visiting www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at https://www.annualcreditreport.com/manualRequestForm.action.

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is as follows:

Equifax
1-866-349-5191
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374

Experian
1-888-397-3742
www.experian.com
P.O. Box 2002
Allen, TX 75013

TransUnion
1-800-888-4213
www.transunion.com
P.O. Box 2000
Chester, PA 19016

Fraud Alerts: You may want to consider placing a fraud alert on your credit report. A fraud alert is free and will stay on your credit report for one (1) year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at www.annualcreditreport.com.

Credit and Security Freezes: You may have the right to place a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax Security Freeze
1-888-298-0045
www.equifax.com
P.O. Box 105788
Atlanta, GA 30348

Experian Security Freeze
1-888-397-3742
www.experian.com
P.O. Box 9554
Allen, TX 75013

TransUnion Security Freeze
1-888-909-8872
www.transunion.com
P.O. Box 160
Woodlyn, PA 19094

This notification was not delayed by law enforcement.

Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.pdf, or by requesting information in writing from the Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

Iowa Residents: Iowa residents can contact the Office of the Attorney general to obtain information about steps to take to avoid identity theft from the Iowa Attorney General's office at: Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines IA 50319, 515-281-5164.

Maryland Residents: Maryland residents can contact the Office of the Attorney General to obtain information about steps you can take to avoid identity theft from the Maryland Attorney General's office at: Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202, (888) 743-0023, http://www.marylandattorneygeneral.gov/.

New York State Residents: New York residents can obtain information about preventing identity theft from the New York Attorney General's Office at: Office of the Attorney General for the State of New York, Bureau of Consumer Frauds & Protection, The Capitol, Albany, New York 12224-0341; https://ag.ny.gov/consumer-frauds/identity-theft; (800) 771-7755.

North Carolina Residents: North Carolina residents can obtain information about preventing identity theft from the North Carolina Attorney General's Office at: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; www.ncdoj.gov.

Rhode Island Residents: We believe that this incident affected one (1) Rhode Island resident. Rhode Island residents can contact the Office of the Attorney general at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov. You have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

Vermont Residents: If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).