

1 Cristina Perez Hesano (#027023)  
2 cperez@perezlawgroup.com  
3 **PEREZ LAW GROUP, PLLC**  
4 7508 N. 59th Avenue  
5 Glendale, AZ 85301  
6 Telephone: 602.730.7100  
7 Fax: 623.235.6173

8 William B. Federman\*  
9 wbf@federmanlaw.com  
10 **FEDERMAN & SHERWOOD**  
11 10205 N. Pennsylvania Ave.  
12 Oklahoma City, OK 73120  
13 Telephone: (405) 235-1560  
14 Fax: (405) 239-2112

15 \*Pro Hac Vice application to be submitted

16 ***Counsel for Plaintiff and the Proposed Class***

17 **UNITED STATES DISTRICT COURT**  
18 **DISTRICT OF ARIZONA**

19 Daniel Davila, individually and on  
20 behalf of all similarly situated persons,

21 Plaintiff,

22 v.

23 New Enchantment Group, LLC,

24 Defendant.

Case No.:

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

25 Plaintiff Daniel Davila, (“Plaintiff”) individually and on behalf of all others  
26 similarly situated, brings this class action lawsuit against Defendant New Enchantment  
27  
28

1 Group, LLC (“Defendant” or “NEG”). The following allegations are based on Plaintiff’s  
2 knowledge, investigation of counsel, facts of public record, and information and belief.

3  
4 I. **NATURE OF THE ACTION**

5 1. Plaintiff seeks to hold NEG,—a limited liability company that develops and  
6 manages resorts, spas, and golf courses,—responsible for the injuries it inflicted on  
7 Plaintiff and approximately **5,568** similarly situated persons ( the “Class” or “Class  
8 Members”).<sup>1</sup> NEG was negligent in maintaining its data security and cybersecurity  
9 training and maintenance. This inadequacy and negligence led to a data breach (“Data  
10 Breach” or “Breach”). Because of NEG’s negligence and inadequate cyber and data  
11 security, Plaintiff’s and Class Members’ highly sensitive and confidential personal  
12 information was exposed to cybercriminals.  
13  
14

15 2. The data that NEG exposed to cybercriminals was highly sensitive. The  
16 exposed data included (at least) personal identifying information (“PII”) like Social  
17 Security Numbers, names, driver’s license numbers, financial account numbers or  
18 credit/debit card numbers (in combination with security codes, access codes, passwords,  
19 or pins for the account).<sup>2</sup> The data exposed also included protected health information  
20 (“PHI”) like health insurance information.<sup>3</sup>  
21  
22  
23  
24

25 <sup>1</sup> See <https://www.mass.gov/doc/assigned-data-breach-number-29112-new-enchantment-group-llc/download>.

26 <sup>2</sup> *Id.*; see also <https://apps.web.maine.gov/online/aevviewer/ME/40/30046e47-1276-423e-99c3-0669e44e44ef.shtml>.

27  
28 <sup>3</sup> See <https://ago.vermont.gov/sites/ago/files/2023-03/2023-02-28%20New%20Enchantment%20Group%20Data%20Breach%20Notice%20to%20Consumers.pdf>.

1           3.       NEG collected PII and PHI (collectively, the “Private Information”) and  
2 then maintained that sensitive data in a negligent and/or reckless manner. As evidenced  
3 by the Data Breach, NEG negligently and inadequately maintained its network—rendering  
4 it easy prey for cybercriminals.  
5

6           4.       According to information and belief, the risk of the Data Breach was known  
7 to NEG. Thus, NEG was on notice that its inadequate data security created a heightened  
8 risk of exposure, compromise, and theft.  
9

10          5.       After the Data Breach, NEG failed to provide timely notice to the exposed  
11 Plaintiff and Class Members—thereby exacerbating their injuries. NEG’s dilatory notice  
12 deprived Plaintiff and Class Members of the chance to take speedy measures to protect  
13 themselves and mitigate harm. Simply put, NEG impermissibly left Plaintiff and Class  
14 Members in the dark—thereby causing their injuries to fester and the damage to spread.  
15

16          6.       Even when NEG finally notified Plaintiff and Class Members of their  
17 exposure, NEG failed to adequately describe what information was compromised.  
18

19          7.       Today, the identities of Plaintiff and Class Members are in jeopardy—all  
20 due to NEG’s negligence. Specifically, Plaintiff and Class Members now suffer from a  
21 present and continuing risk of fraud and identity theft. And now, Plaintiff and Class  
22 Members must constantly monitor their credit reports and financial accounts.  
23

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

1 individual health needs, use Class Members’ identities to obtain government benefits, file  
2 fraudulent tax returns using Class Members’ information, obtain driver’s licenses in Class  
3 Members’ names (but with another person’s photograph), and give false information to  
4 police during an arrest.  
5

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

10 10. Plaintiff and Class Members have suffered—and will continue to suffer—  
11 from the loss of the benefit of their bargain, unexpected out-of-pocket expenses, lost or  
12 diminished value of their Private Information, emotional distress, and the value of their  
13 time reasonably incurred to mitigate the fallout of the NEG’s Data Breach.  
14

15 11. Through this action, Plaintiff seeks to remedy these injuries on behalf of  
16 himself and all similarly situated individuals whose Private Information was exposed and  
17 compromised in the Data Breach.  
18

19 12. Plaintiff seeks remedies including, but not limited to, compensatory  
20 damages, treble damages, punitive damages, reimbursement of out-of-pocket costs, and  
21 injunctive relief—including improvements to NEG’s data security systems, future annual  
22 audits, and adequate credit monitoring services funded by NEG.  
23

24 13. Plaintiff brings this action against NEG and asserts claims for: (1)  
25 negligence, (2) breach of implied contract, (3) unjust enrichment, and (4) violations of  
26 Arizona’s Consumer Fraud Act.  
27  
28

1 **PARTIES**

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

7  
8 15. Defendant **New Enchantment Group, LLC** is a Delaware limited liability  
9 company, registered as a foreign LLC in the State of Arizona, with its principal place of  
10 business at 16430 N. Scottsdale Rd., Suite 115, Scottsdale, Arizona, 85254.

11 **JURISDICTION AND VENUE**

12  
13 16. This Court has original jurisdiction under the Class Action Fairness Act, 28  
14 U.S.C. § 1332(d)(2), because this is a class action involving more than 100 putative class  
15 members and the amount in controversy exceeds \$5,000,000, exclusive of interest and  
16 costs. And minimal diversity is established because, upon information and belief, many  
17 members of the Class are citizens of states different than Defendant’s.

18  
19 17. This Court has general personal jurisdiction over NEG because NEG’s  
20 principal place of business and headquarters are in Scottsdale, Arizona. NEG regularly  
21 conducts substantial business in and from Arizona.

22  
23 18. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2),  
24 and 1391(c)(2) because substantial events giving rise to the claims emanated from  
25 activities within this District, and NEG conducts substantial business in this District.  
26  
27  
28

---

<sup>4</sup> 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.<sup>5</sup> In connection with the development and management of these properties, NEG receives certain information belonging to resort employees and other individuals.<sup>6</sup> 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.

---

<sup>5</sup> 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>.

<sup>6</sup> *Id.*

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

3           23. On information and belief, NEG acquired, *inter alia*, the following types of  
4 information: Social Security Numbers, names, driver's license numbers, financial account  
5 numbers or credit/debit card numbers (in combination with security codes, access codes,  
6 passwords, or pins for the account) and health insurance information.  
7

8           24. By obtaining, collecting, and storing Plaintiff's and Class Members' Private  
9 Information, NEG assumed legal and equitable duties and knew, or should have known,  
10 that it was thereafter responsible for protecting Plaintiff's and Class Members' Private  
11 Information from unauthorized disclosure.  
12

13           25. Upon information and belief, Plaintiff and Class Members relied on NEG  
14 to keep their Private Information confidential and securely maintained, to use this  
15 information for business and employment purposes only, and to make only authorized  
16 disclosures of this information.  
17

18           26. NEG could have prevented the Data Breach by properly securing and  
19 encrypting and/or more securely encrypting its servers generally, as well as Plaintiff's  
20 and Class Members' Private Information.  
21

22           27. NEG's negligence in safeguarding Plaintiff's and Class Members'  
23 Private Information was exacerbated by repeated warnings and alerts directed to the  
24 increased need to protect and secure sensitive data, as evidenced by the trending data breach  
25 attacks in recent years.  
26  
27  
28

1 28. Despite the prevalence of public announcements of data breaches and  
2 data security compromises, NEG failed to take appropriate steps to protect Plaintiff's  
3 and Class Members' Private Information from being compromised.  
4

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

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

8 31. NEG failed to ensure file integrity.

9 32. NEG failed to properly train its employees as to cybersecurity awareness  
10 and best practices, specifically, how to avoid, detect, and report email phishing attacks.  
11

12 33. NEG failed to provide fair, reasonable, or adequate computer systems and  
13 data security practices to safeguard the Private Information of Plaintiff and Class  
14 Members.  
15

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

18 35. NEG knowingly disregarded standard information security principles,  
19 despite obvious risks, by allowing unmonitored and unrestricted access to unsecured  
20 Private Information.  
21

22 36. NEG failed to provide adequate supervision and oversight of the Private  
23 Information with which it was and is entrusted, despite the known risk and foreseeable  
24 likelihood of breach and misuse, which permitted an unknown third party to gather Private  
25 Information of Plaintiff and Class Members, misuse the Private Information and  
26 potentially disclose it to others without consent.  
27  
28



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

3 38. According to information and belief, NEG failed to adequately train its  
4 employees to not store Private Information longer than absolutely necessary.  
5

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

8 40. Upon information and belief, NEG failed to consistently enforce security  
9 policies aimed at protecting Plaintiff's and the Class Members' Private Information.  
10

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

13 42. Upon information and belief, NEG failed to encrypt Plaintiff's and Class  
14 Members' Private Information and monitor user behavior and activity to identify possible  
15 threats.  
16

17 ***NEG's Data Breach***

18 43. On October 4, 2022, NEG discovered unusual activity on its systems and  
19 determined that certain data had been encrypted by a third-party.<sup>7</sup> NEG discovered that  
20 cybercriminals had unrestricted access to its files and systems from October 3, 2022, to  
21 October 4, 2022.<sup>8</sup>  
22

23 44. After an investigation, NEG admitted that "the unknown third party  
24 ***accessed and acquired*** certain documents from [its] systems during this period."<sup>9</sup> Based  
25

26 \_\_\_\_\_  
27 <sup>7</sup> *Id.*

28 <sup>8</sup> *Id.*

<sup>9</sup> *Id.* (emphasis added).

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

3  
4 45. On information and belief, cybercriminals were able to breach NEG’s  
5 systems because NEG did not maintain reasonable security safeguards or protocols to  
6 protect Plaintiff’s and the Class’s Private Information, leaving it an unguarded target for  
7 theft and misuse. NEG admits as much in its Notice Letter sent to victims, admitting that  
8 after the fact: “we have taken steps to reduce the risk of this type of incident occurring in  
9 the future, including enhancing or technical security measures.”<sup>10</sup>  
10

11 46. Simply put, Defendant should have implemented those enhanced “technical  
12 security measures” years ago—thereby preventing the Data Breach and all of Plaintiff and  
13 Class Members’ injuries.  
14

15 47. While NEG claims to have become aware of the Data Breach as early as  
16 October 4, 2022, NEG delayed notifying victims of the Data Breach. NEG completed a  
17 review of the documents acquired during the Data Breach on December 9, 2022, but did  
18 not begin issuing Notice of Data Breach letters until in or around February 2023.<sup>11</sup>  
19 Shockingly, on April 5, 2023, NEG revealed *additional documents* were acquired by the  
20 cybercriminals during the Data Breach and sent out *another* batch of Notice of Data  
21 Breach letters on or around May 6, 2023.<sup>12</sup> NEG has no valid excuse for delaying notice  
22  
23  
24

---

25 <sup>10</sup> *Id.*

26 <sup>11</sup> *Id.*

27 <sup>12</sup> *See Exhibit 1* (Plaintiff’s Notice of Data Breach Letter).  
28

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

3  
4 48. Time is of the essence when highly sensitive Private Information is subject  
5 to unauthorized access and/or acquisition. The disclosed, accessed, and acquired Private  
6 Information of Plaintiff and Class Members is likely available on the Dark Web. Hackers  
7 can access and then offer for sale the unencrypted, unredacted Private Information to  
8 criminals. Plaintiff and Class Members are now subject to the present and continuing risk  
9 of fraud, identity theft, and misuse resulting from the possible publication of their Private  
10 Information, especially their Social Security Numbers onto the Dark Web. Plaintiff and  
11 Class Members now face a lifetime risk of identity theft, which is heightened here by  
12 unauthorized access, theft, and/or disclosure of thousands of Social Security Numbers.  
13

14  
15 49. Following the Breach, and recognizing that each Class Member is now  
16 subject to the present and continuing risk of identity theft and fraud, NEG’s Notice of Data  
17 Breach Letter encouraged Plaintiff and the Class to “take advantage” of the measly one  
18 (1) year of credit monitoring offered to Plaintiff and the Class. Such measures are  
19 insufficient to protect Plaintiff and Class Members from the lifetime risks each now face.  
20 As another element of damages, Plaintiff and Class Members seek a sum of money  
21 sufficient to provide to Plaintiff and Class Members identity theft protective services for  
22 their respective lifetimes.  
23  
24  
25  
26  
27  
28

1 50. Time is a compensable and valuable resource in the United States.  
2 According to the U.S. Bureau of Labor Statistics, 55.5% of U.S.-based workers are  
3 compensated on an hourly basis, while the other 44.5% are salaried.<sup>13</sup>  
4

5 51. According to the U.S. Bureau of Labor Statistics' 2018 American Time Use  
6 Survey, American adults have only 36 to 40 hours of "leisure time" outside of work per  
7 week;<sup>14</sup> leisure time is defined as time not occupied with work or chores and is "the time  
8 equivalent of 'disposable income.'"<sup>15</sup> Usually, this time can be spent at the option and  
9 choice of the consumer, however, having been notified of the Data Breach, consumers  
10 now have to spend hours of their leisure time self-monitoring their accounts,  
11 communicating with financial institutions and government entities, and placing other  
12 prophylactic measures in place to attempt to protect themselves.  
13  
14

15 52. Plaintiff and Class Members are now deprived of the choice as to how to  
16 spend their valuable free hours and seek renumeration for the loss of valuable time as  
17 another element of damages.  
18  
19  
20

---

21 <sup>13</sup> *Characteristics of minimum wage workers, 2020*, U.S. BUREAU OF LABOR STATISTICS  
22 [https://www.bls.gov/opub/reports/minimum-wage/2020/home.htm#:~:text=](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%20Weekly%20Wage%20Data)  
23 *Average Weekly Wage Data*, U.S. BUREAU OF LABOR STATISTICS, *Average Weekly*  
24 *Wage Data*, [https://data.bls.gov/cew/apps/table\\_maker/v4/](https://data.bls.gov/cew/apps/table_maker/v4/table_maker.htm%23type=1&year=2021&qtr=3&own=5&ind=10&supp=0)  
25 [table\\_maker.htm%23type=1&year=2021&qtr=3&own=5&ind=10&supp=0](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  
26 accessed Aug. 2, 2022) (finding that on average, private-sector workers make \$1,253 per  
27 40-hour work week.).

28 <sup>14</sup> 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).

<sup>15</sup> *Id.*

1           53. Upon information and belief, the unauthorized third-party cybercriminals  
2 gained access to Plaintiff's and Class Members' Private Information with the intent of  
3 engaging in misuse of the Private Information and financial information, including  
4 marketing, and selling Plaintiff's and Class Members' Private Information.  
5

6           54. NEG had and continues to have obligations created by reasonable industry  
7 standards, common law, state statutory law, and its own assurances and  
8 representations to keep Plaintiff's and Class Members' Private Information confidential  
9 and to protect such Private Information from unauthorized access.  
10

11           55. NEG's Breach Notice letter omits the size and scope of the breach. NEG has  
12 demonstrated a pattern of providing inadequate notices and disclosures about the Data  
13 Breach (as evidenced by the two separate batches of Notice of Data Breach Letters).  
14

15           56. Plaintiff and the Class Members remain, even today, are in the dark  
16 regarding what particular data was stolen, the particular ransomware used, and what steps  
17 are being taken, if any, to secure their Private Information going forward. Plaintiff  
18 and Class Members are left to speculate as to the full impact of the Data Breach and how  
19 exactly NEG intends to enhance its information security systems and monitoring  
20 capabilities so as to prevent further breaches.  
21

22           57. Plaintiff's and Class Members' Private Information and financial  
23 information may end up for sale on the dark web, or simply fall into the hands of  
24 companies that will use the detailed Private Information for targeted marketing without  
25 the approval of Plaintiff and/or Class Members. Either way, unauthorized individuals  
26 can now easily access the Private Information of Plaintiff and Class Members.  
27

28           ***NEG Failed to Comply with FTC Guidelines***

1           58. According to the Federal Trade Commission (“FTC”), the need for data  
2 security should be factored into all business decision-making.<sup>16</sup> To that end, the FTC has  
3 issued numerous guidelines identifying best data security practices that businesses, such  
4 as NEG, should employ to protect against the unlawful exposure of Personal Information.  
5

6           59. In 2016, the FTC updated its publication, *Protecting Personal Information:*  
7 *A Guide for Business*, which established guidelines for fundamental data security  
8 principles and practices for business.<sup>17</sup> The guidelines explain that businesses should:  
9

- 10           a. protect the personal customer information that they keep;
- 11           b. properly dispose of personal information that is no longer needed;
- 12           c. encrypt information stored on computer networks;
- 13           d. understand their network’s vulnerabilities; and
- 14           e. implement policies to correct security problems.

15           60. The guidelines also recommend that businesses watch for large amounts of  
16 data being transmitted from the system and have a response plan ready in the event of a  
17 breach.  
18

19           61. The FTC recommends that companies not maintain Private Information  
20 longer than is needed for authorization of a transaction; limit access to sensitive data;  
21 require complex passwords to be used on networks; use industry-tested methods for  
22  
23  
24  
25

---

26 <sup>16</sup> *Start with Security: A Guide for Business*, FED. TRADE COMM’N (June 2015),  
27 <https://bit.ly/3uSoYWF>.

28 <sup>17</sup> *Protecting Personal Information: A Guide for Business*, FED. TRADE COMM’N (Oct.  
2016), <https://bit.ly/3u9mzre>.

1 security; monitor for suspicious activity on the network; and verify that third-party service  
2 providers have implemented reasonable security measures.<sup>18</sup>

3  
4 62. The FTC has brought enforcement actions against businesses for failing to  
5 adequately and reasonably protect customer data, treating the failure to employ reasonable  
6 and appropriate measures to protect against unauthorized access to confidential consumer  
7 data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission  
8 Act (“FTCA”), 15 U.S.C. § 45. Orders resulting from these actions further clarify the  
9 measures businesses must take to meet their data security obligations.  
10

11 63. NEG’s failure to employ reasonable and appropriate measures to protect  
12 against unauthorized access to the Private Information constitutes an unfair act or practice  
13 prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.  
14

15 ***NEG Failed to Follow Industry Standards***

16 64. NEG failed to meet the minimum standards of any of the following  
17 frameworks: the NIST Cybersecurity Framework Version 1.1 (including without  
18 limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1,  
19 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  
20 RS.CO-2), and the Center for Internet Security’s Critical Security Controls (CIS CSC),  
21 which are all established standards in reasonable cybersecurity readiness.  
22

23 65. Such frameworks are the existing and applicable industry standards. And  
24 NEG failed to comply with these accepted standards—thus opening the door to criminals  
25 and the Data Breach.  
26

27  
28  

---

<sup>18</sup> 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*.<sup>19</sup> 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

---

<sup>19</sup> See **Exhibit 1** (Plaintiff’s Notice of Data Breach Letter).



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

3  
4 71. Plaintiff entrusted their Private Information to NEG. By accepting Plaintiff's  
5 and the Class's PII it undertook the obligation and duty to protect and maintain the  
6 confidentiality of Private Information entrusted to it. Thus, Plaintiff had the reasonable  
7 expectation and understanding that NEG would take—*at minimum*—industry standard  
8 precautions to protect, maintain, and safeguard that information from unauthorized users  
9 or disclosure, and would timely notify them of any data security incidents. After all,  
10 Plaintiff would not have entrusted his Private Information to NEG had he known that NEG  
11 would not take reasonable steps to safeguard his information.  
12

13  
14 72. Plaintiff suffered actual injury from having his Private Information  
15 compromised because of the Data Breach including, but not limited to (a) damage to and  
16 diminution in the value of his Private Information—a form of property that NEG obtained  
17 from Plaintiff; (b) violation of his privacy rights; (c) the theft of his Private Information;  
18 (d) lost time spent investigating and addressing the effects of the Data Breach; (e) out of  
19 pocket expenses for credit monitoring; and/or (f) present and continuing injury arising  
20 from the present and continuing risk of identity theft and fraud.  
21

22  
23 73. As a result of the Data Breach, Plaintiff also suffered emotional distress  
24 because of the release of his Private Information—which he believed would be protected  
25 from unauthorized access and disclosure. Now, Plaintiff suffers from anxiety about  
26 unauthorized parties viewing, selling, and/or using his Private Information for nefarious  
27 purposes like identity theft and fraud.  
28

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

3           75. Because of the Data Breach, Plaintiff has spent—and will continue to  
4 spend—considerable time and money to try to mitigate and address harms caused by the  
5 Data Breach.  
6

7           ***Plaintiff's Experience***

8           76. Plaintiff Davila was an employee of NEG and provided his Private  
9 Information to NEG to receive employment and/or elective benefits.  
10

11           77. Plaintiff entrusted his Private Information to NEG with the reasonable  
12 expectation and understanding that NEG would take at a minimum, industry standard  
13 precautions to protect, maintain, and safeguard that information from unauthorized users  
14 or disclosure, and would timely notify him of any data security incidents related to him.  
15 Plaintiff would not have used NEG's services and/or accepted employment had he known  
16 that NEG would not take reasonable steps to safeguard his Private Information.  
17

18           78. In or around June 8, 2023, Plaintiff received a Notice of Data Breach Letter  
19 from NEG, notifying him that his name, Social Security Number, and health insurance  
20 information had been improperly accessed and obtained by unauthorized cybercriminals.  
21

22           79. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate  
23 the impact of the Data Breach after receiving the Notice of Data Breach Letter, including  
24 but not limited to researching the Data Breach and reviewing credit card and financial  
25 account statements.  
26  
27  
28

1           80. Plaintiff has spent a few hours and will continue to spend valuable time he  
2 otherwise would have spent on other activities, including but not limited to work and/or  
3 recreation.  
4

5           81. Plaintiff suffered actual injury from having his Private Information  
6 compromised as a result of the Data Breach including, but not limited to (a) damage to  
7 and diminution in the value of his Private Information, a form of property that NEG  
8 obtained from Plaintiff; (b) violation of his privacy rights; (b) the theft of his Private  
9 Information; and (d) imminent and impending injury arising from the increased risk of  
10 identity theft and fraud.  
11

12           82. As a result of the Data Breach, Plaintiff has also suffered emotional distress  
13 as a result of the release of his Private Information, which he believed would be protected  
14 from unauthorized access and disclosure, including anxiety about unauthorized parties  
15 viewing, selling, and/or using his Private Information for purposes of identity theft and  
16 fraud. Plaintiff is very concerned about identity theft and fraud, as well as the  
17 consequences of such identity theft and fraud resulting from the Data Breach. Plaintiff  
18 also has suffered anxiety about unauthorized parties viewing, using, and/or publishing his  
19 information.  
20  
21

22           83. As a result of the Data Breach, Plaintiff anticipates spending considerable  
23 time and money on an ongoing basis to try to mitigate and address harms caused by the  
24 Data Breach. In addition, Plaintiff will continue to be at present, imminent, and continued  
25 increased risk of identity theft and fraud for years to come.  
26  
27  
28

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

3            84. Plaintiff and Class Members suffered injury from the misuse of their Private  
4 Information that can be directly traced to NEG.  
5

6            85. The ramifications of NEG's failure to keep Plaintiff's and the Class's Private  
7 Information secure are severe. Identity theft occurs when someone uses another's personal  
8 and financial information such as that person's name, account number, Social Security  
9 Number, driver's license number, date of birth, and/or other information, without  
10 permission, to commit fraud or other crimes.  
11

12            86. According to experts, one out of four data breach notification recipients  
13 become a victim of identity fraud.<sup>20</sup>  
14

15            87. As a result of NEG's failures to prevent—and to timely detect—the Data  
16 Breach, Plaintiff and Class Members suffered and will continue to suffer damages,  
17 including monetary losses, lost time, anxiety, and emotional distress. They have suffered  
18 or are at a present risk of suffering:  
19

- 20            a. The loss of the opportunity to control how their Private Information is used;  
21            b. The diminution in value of their Private Information;  
22            c. The compromise and continuing publication of their Private Information;  
23            d. Out-of-pocket costs associated with the prevention, detection, recovery, and  
24 remediation from identity theft or fraud;  
25

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

- 1 e. Lost opportunity costs and lost wages associated with the time and effort
- 2 expended addressing and attempting to mitigate the actual and future consequences
- 3 of the Data Breach, including, but not limited to, efforts spent researching how to
- 4 prevent, detect, contest, and recover from identity theft and fraud;
- 5
- 6 f. Delay in receipt of tax refund monies;
- 7
- 8 g. Unauthorized use of stolen Private Information; and
- 9
- 10 h. The continued risk to their Private Information, which remains in the
- 11 possession of NEG and is subject to further breaches so long as NEG fails to
- 12 undertake the appropriate measures to protect the Private Information in its
- 13 possession.

14 88. Stolen Private Information is one of the most valuable commodities on the

15 criminal information black market. According to Experian, a credit-monitoring service,

16 stolen Private Information can be worth up to \$1,000.00 depending on the type of

17 information obtained.<sup>21</sup>

18 89. The value of Plaintiff’s and the proposed Class’s Private Information on the

19 black market is considerable. Stolen Private Information trades on the black market for

20 years, and criminals frequently post stolen private information openly and directly on

21 various “dark web” internet websites, making the information publicly available, for a

22 substantial fee of course.

23

24

25

26

---

27 <sup>21</sup> Brian Stack, *Here’s How Much Your Personal Information Is Selling for on the Dark*

28 *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/>.

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

3           91. One such example of criminals using Private Information for profit is the  
4 development of “Fullz” packages.<sup>22</sup>

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

9           93. The development of “Fullz” packages means that stolen Private Information  
10 from the Data Breach can easily be used to link and identify it to Plaintiff’s and the  
11 proposed Class’s phone numbers, email addresses, and other unregulated sources and  
12 identifiers. In other words, even if certain information such as emails, phone numbers, or  
13 credit card numbers may not be included in the Private Information stolen by the cyber-  
14 criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a  
15 higher price to unscrupulous operators and criminals (such as illegal and scam  
16  
17  
18  
19  
20

---

21 <sup>22</sup> “Fullz” is fraudster speak for data that includes the information of the victim, including,  
22 but not limited to, the name, address, credit card information, Social Security Number,  
23 date of birth, and more. As a rule of thumb, the more information you have on a victim,  
24 the more money can be made off those credentials. Fullz are usually pricier than standard  
25 credit card credentials, commanding up to \$100 per record or more on the dark web. Fullz  
26 can be cashed out (turning credentials into money) in various ways, including performing  
27 bank transactions over the phone with the required authentication details in-hand. Even  
28 “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/>.

1 telemarketers) over and over. That is exactly what is happening to Plaintiff and members  
2 of the proposed Class, and it is reasonable for any trier of fact, including this Court or a  
3 jury, to find that Plaintiff's and other members of the proposed Class's stolen Private  
4 Information is being misused, and that such misuse is fairly traceable to the Data Breach.  
5

6 94. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet  
7 Crime Report, Internet-enabled crimes reached their highest number of complaints and  
8 dollar losses that year, resulting in more than \$3.5 billion in losses to individuals and  
9 business victims.  
10

11 95. Further, according to the same report, "rapid reporting can help law  
12 enforcement stop fraudulent transactions before a victim loses the money for good." NEG  
13 did not rapidly report to Plaintiff and the Class that their Private Information had been  
14 stolen.  
15

16 96. Victims of identity theft also often suffer embarrassment, blackmail, or  
17 harassment in person or online, and/or experience financial losses resulting from  
18 fraudulently opened accounts or misuse of existing accounts.  
19

20 97. In addition to out-of-pocket expenses that can exceed thousands of dollars  
21 and the emotional toll identity theft can take, some victims have to spend a considerable  
22 time repairing the damage caused by the theft of their Private Information. Victims of new  
23 account identity theft will likely have to spend time correcting fraudulent information in  
24 their credit reports and continuously monitor their reports for future inaccuracies, close  
25 existing bank/credit accounts, open new ones, and dispute charges with creditors.  
26

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

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

3  
4 99. The Federal Trade Commission (“FTC”) has also recognized that consumer  
5 data is a new and valuable form of currency. In an FTC roundtable presentation, former  
6 Commissioner Pamela Jones Harbour stated that “most consumers cannot begin to  
7 comprehend the types and amount of information collected by businesses, or why their  
8 information may be commercially valuable. Data is currency.”<sup>23</sup>

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

---

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

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

28 <sup>25</sup> *Id.*



1           101. According to the FTC, unauthorized Private Information disclosures are  
2 extremely damaging to consumers’ finances, credit history and reputation, and can take  
3 time, money, and patience to resolve the fallout.<sup>26</sup> The FTC treats the failure to employ  
4 reasonable and appropriate measures to protect against unauthorized access to confidential  
5 consumer data as an unfair act or practice prohibited by Section 5(a) of the FTC Act (the  
6 “FTCA”).  
7

8           102. To that end, the FTC has issued orders against businesses that failed to  
9 employ reasonable measures to secure sensitive payment card data. *See In the matter of*  
10 *Lookout Services, Inc.*, No. C-4326, ¶ 7 (June 15, 2011) (“[Defendant] allowed users to  
11 bypass authentication procedures” and “failed to employ sufficient measures to detect and  
12 prevent unauthorized access to computer networks, such as employing an intrusion  
13 detection system and monitoring system logs.”); *In the matter of DSW, Inc.*, No. C-4157,  
14 ¶ 7 (Mar. 7, 2006) (“[Defendant] failed to employ sufficient measures to detect  
15 unauthorized access.”); *In the matter of The TJX Cos., Inc.*, No. C-4227 (Jul. 29, 2008)  
16 (“[R]espondent stored . . . personal information obtained to verify checks and process  
17 unreceipted returns in clear text on its in-store and corporate networks[,]” “did not require  
18 network administrators . . . to use different passwords to access different programs,  
19 computers, and networks[,]” and “failed to employ sufficient measures to detect and  
20 prevent unauthorized access to computer networks . . .”); *In the matter of Dave & Buster’s*  
21 *Inc.*, No. C-4291 (May 20, 2010) (“[Defendant] failed to monitor and filter outbound  
22  
23  
24  
25  
26  
27

28 <sup>26</sup> *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>.

1 traffic from its networks to identify and block export of sensitive personal information  
2 without authorization” and “failed to use readily available security measures to limit  
3 access between instore networks . . .”). These orders, which all preceded the Data Breach,  
4 further clarify the measures businesses must take to meet their data security obligations.  
5  
6 NEG thus knew or should have known that its data security protocols were inadequate and  
7 were likely to result in the unauthorized access to and/or theft of Private Information.

8  
9 103. Over the past several years, data breaches have become alarmingly  
10 commonplace. In 2016, the number of data breaches in the U.S. exceeded 1,000, a 40%  
11 increase from 2015.<sup>27</sup> The next year, that number increased by nearly 45%.<sup>28</sup>

12 104. Charged with handling highly sensitive Personal Information including  
13 health insurance information, Social Security numbers, and financial information, NEG  
14 knew or should have known the importance of safeguarding the Personal Information that  
15 was entrusted to it. NEG also knew or should have known of the foreseeable consequences  
16 if its data security systems were breached. This includes the significant costs that would  
17 be imposed on NEG’s employees and customers because of a breach. NEG nevertheless  
18 failed to take adequate cybersecurity measures to prevent the Data Breach from occurring.  
19  
20

21 105. NEG disclosed the Private Information of Plaintiff and members of the  
22 proposed Class for criminals to use in the conduct of criminal activity. Specifically, NEG  
23 opened, disclosed, and exposed the Private Information of Plaintiff and members of the  
24

---

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

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

1 proposed Class to people engaged in disruptive and unlawful business practices and  
2 tactics, including online account hacking, unauthorized use of financial accounts, and  
3 fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using  
4 the stolen Private Information.  
5

6 106. NEG's use of outdated and insecure computer systems and software that are  
7 easy to hack, and its failure to maintain adequate security measures and an up-to-date  
8 technology security strategy, demonstrates a willful and conscious disregard for privacy,  
9 and has exposed the Private Information of Plaintiff and potentially thousands of members  
10 of the proposed Class to unscrupulous operators, con artists, and outright criminals. NEG  
11 certainly knew, or should have known, that entities harboring Private Information are  
12 particularly vulnerable to cyberattacks and that, as a result, it must take steps to protect  
13 the trove of Private Information it holds.  
14  
15

16 107. Yet, on information and belief, NEG failed to implement even the most basic  
17 levels of cybersecurity.  
18

19 108. NEG's failure to properly notify Plaintiff and members of the proposed  
20 Class of the Data Breach then exacerbated Plaintiff's and members of the proposed Class's  
21 injury by depriving them of the earliest ability to take appropriate measures to protect their  
22 Private Information and take other necessary steps to mitigate the harm caused by the Data  
23 Breach.  
24

25 **CLASS ACTION ALLEGATIONS**

26 109. Plaintiff brings this action on behalf of themselves and on behalf of all other  
27 persons similarly situated ("the Class") under Fed. R. Civ. P. 23(b)(2), 23(b)(3), and  
28 23(c)(4).

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

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

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

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

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

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

21 115. **Numerosity**. The Class Members are numerous such that joinder is  
22 impracticable. While the exact number of Class Members is unknown to Plaintiff at this  
23  
24  
25  
26  
27  
28

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

3  
4 116. **Commonality**. There are many questions of law and fact common to the  
5 Classes. And these common questions predominate over any individualized questions of  
6 individual Class Members. These common questions of law and fact include, without  
7 limitation:

- 8 a. If NEG unlawfully maintained, lost, or disclosed Plaintiff’s and Class  
9 Members’ Private Information;
- 10 b. If NEG failed to implement and maintain reasonable security procedures and  
11 practices appropriate to the nature and scope of the information  
12 compromised in the Data Breach;
- 13 c. If NEG’s data security systems prior to and during the Data Breach complied  
14 with applicable data security laws and regulations including;
- 15 d. If NEG’s data security systems prior to and during the Data Breach were  
16 consistent with industry standards;
- 17 e. If NEG owed a duty to Class Members to safeguard their Private  
18 Information;
- 19 f. If NEG breached its duty to Class Members to safeguard their Private  
20 Information;
- 21 g. If NEG knew or should have known that its data security systems and  
22 monitoring processes were deficient;
- 23 h. If NEG should have discovered the Data Breach earlier;
- 24  
25  
26  
27  
28

- 1 i. If NEG took reasonable measures to determine the extent of the Data Breach
- 2 after it was discovered;
- 3 j. If NEG’s delay in informing Plaintiff and Class Members of the Data Breach
- 4 was unreasonable;
- 5 k. If NEG’s method of informing Plaintiff and Class Members of the Data
- 6 Breach was unreasonable;
- 7 l. If NEG’s conduct was negligent;
- 8 m. If Plaintiff and Class Members were injured as a proximate cause or result
- 9 of the Data Breach;
- 10 n. If Plaintiff and Class Members suffered legally cognizable damages as a
- 11 result of NEG’s misconduct;
- 12 o. If NEG breached implied contracts with Plaintiff and Class Members;
- 13 p. If NEG violated the consumer protection statutes invoked herein;
- 14 q. If NEG was unjustly enriched by unlawfully retaining a benefit conferred
- 15 upon it by Plaintiff and Class Members;
- 16 r. If NEG failed to provide notice of the Data Breach in a timely manner, and;
- 17 s. If Plaintiff and Class Members are entitled to damages, civil penalties,
- 18 punitive damages, treble damages, and/or injunctive relief.
- 19
- 20
- 21
- 22
- 23
- 24
- 25
- 26
- 27
- 28

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.

1           118. **Adequacy of Representation**. Plaintiff will fairly and adequately represent  
2 and protect the interests of the Members of the Classes. Plaintiff’s Counsel are competent  
3 and experienced in litigating complex class actions. Plaintiff has no interests that conflict  
4 with, or are antagonistic to, those of the Classes.  
5

6           119. **Predominance**. NEG has engaged in a common course of conduct toward  
7 Plaintiff and Class Members, in that all the Plaintiff and Class Members’ data was stored  
8 on the same computer system and unlawfully exposed in the same way. The common  
9 issues arising from NEG’s conduct affecting Class Members set out above predominate  
10 over any individualized issues. Adjudication of these common issues in a single action has  
11 important and desirable advantages of judicial economy.  
12

13           120. **Superiority**. A class action is superior to other available methods for the  
14 fair and efficient adjudication of the controversy. Class treatment of common questions of  
15 law and fact is superior to multiple individual actions or piecemeal litigation. Absent a  
16 class action, most Class Members would likely find that the cost of litigating their  
17 individual claims is prohibitively high and would therefore have no effective remedy. The  
18 prosecution of separate actions by individual Class Members would create a risk of  
19 inconsistent or varying adjudications with respect to individual Class Members, which  
20 would establish incompatible standards of conduct for NEG. In contrast, the conduct of  
21 this action as a Class action presents far fewer management difficulties, conserves judicial  
22 resources, the parties’ resources, and protects the rights of each Class Member.  
23  
24  
25

26           121. The litigation of the claims brought herein is manageable. NEG’s uniform  
27 conduct, the consistent provisions of the relevant laws, and the ascertainable identities of  
28

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

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

5  
6 123. Likewise, particular issues under Rule 23(c)(4) are appropriate for  
7 certification because such claims present only particular, common issues, the resolution  
8 of which would advance the disposition of this matter and the parties' interests therein.  
9 Such particular issues include those set forth above.

10  
11 124. NEG has acted on grounds that apply generally to the Class as a whole, so  
12 that Class certification, injunctive relief, and corresponding declaratory relief are  
13 appropriate on a Class-wide basis.

14  
15 **FIRST CAUSE OF ACTION**  
16 **Negligence**  
**(On Behalf of Plaintiff and the Class)**

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

19  
20 126. NEG required Plaintiff and Class Members, to provide their Private  
21 Information to receive employment, elective benefits, and/or services.

22 127. By collecting and storing this data in its computer system and network for  
23 its own commercial gain, NEG owed a duty of care to use reasonable means to secure and  
24 safeguard its computer system—and Class Members' Private Information held within it—  
25 to prevent disclosure of the information, and to safeguard the information from theft.  
26 NEG's duty included a responsibility to implement processes so it could detect a breach  
27  
28



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

3 128. The risk that unauthorized persons would attempt to gain access to the  
4 Private Information and misuse it was foreseeable. Given that NEG holds vast amounts of  
5 Private Information, it was inevitable that unauthorized individuals would at some point  
6 try to access NEG's databases of Private Information.  
7

8 129. After all, Private Information is highly valuable, and NEG knew, or should  
9 have known, the risk in obtaining, using, handling, emailing, and storing the Private  
10 Information of Plaintiff and Class Members. Thus, NEG knew, or should have known, the  
11 importance of exercising reasonable care in handling the Private Information entrusted to  
12 it.  
13

14 130. NEG owed a duty of care to Plaintiff and Class Members to provide data  
15 security consistent with industry standards and other requirements discussed herein, and  
16 to ensure that its systems and networks, and the personnel responsible for them, adequately  
17 protected the Private Information.  
18

19 131. NEG's duty of care to use reasonable security measures arose because of the  
20 special relationship that existed between NEG, its employees, and its customers, which is  
21 recognized by laws and regulations including the FTC Act, as well as common law. NEG  
22 was in a superior position to ensure that its systems were sufficient to protect against the  
23 foreseeable risk of harm to Class Members from a data breach.  
24

25 132. Under the Federal Trade Commission Act, NEG had a duty to employ  
26 reasonable security measures. Specifically, this statute prohibits "unfair . . . practices in or  
27  
28

1 affecting commerce,” including (as interpreted and enforced by the FTC) the unfair  
2 practice of failing to use reasonable measures to protect confidential data.<sup>29</sup>

3  
4 133. Moreover, Plaintiff and Class Members’ injuries are precisely the type of  
5 injuries that the FTC Act guards against. After all, the FTC has pursued numerous  
6 enforcement actions against businesses that—because of their failure to employ  
7 reasonable data security measures and avoid unfair and deceptive practices—caused the  
8 very same injuries that Defendant inflicted upon Plaintiff and Class Members.  
9

10 134. Under the Arizona Data Breach Notification Act, NEG has a duty to  
11 promptly notify affected persons so they can take action to protect themselves if “the  
12 investigation [of a potential data breach] results in a determination that there has been a  
13 security system breach, the person that owns or licenses the computerized data, within  
14 forty-five days after the determination, shall . . . [n]otify the individuals affected.”<sup>30</sup>  
15

16 135. Moreover, Plaintiff and Class Members’ injuries are precisely the type of  
17 injuries that the Arizona Data Breach Notification Act guards against.  
18

19 136. NEG’s duty to use reasonable care in protecting confidential data arose not  
20 only because of the statutes and regulations described above, but also because NEG is  
21 bound by industry standards to protect confidential Private Information.  
22

23 137. NEG owed Plaintiff and members of the Class a duty to notify them within  
24 a reasonable time frame of any breach to their Private Information. Defendant also owed  
25 a duty to timely and accurately disclose to Plaintiff and members of the Class the scope,  
26 nature, and occurrence of the Data Breach. This duty is necessary for Plaintiff and Class  
27

28 <sup>29</sup> 15 U.S.C. § 45.  
<sup>30</sup> A.R.S §§ 18-551, 18-552.

1 Members to take appropriate measures to protect their Private Information, to be vigilant  
2 in the face of an increased risk of harm, and to take other necessary steps in an effort to  
3 mitigate the fallout of NEG's Data Breach.  
4

5 138. NEG owed these duties to Plaintiff and Class Members because they are  
6 members of a well-defined, foreseeable, and probable class of individuals whom NEG  
7 knew or should have known would suffer injury-in-fact from its inadequate security  
8 protocols. After all, NEG actively sought and obtained the Private Information of Plaintiff  
9 and Class Members.  
10

11 139. NEG breached its duties, and thus was negligent, by failing to use reasonable  
12 measures to protect Class Members' Private Information. And but for NEG's negligence,  
13 Plaintiff and Class Members would not have been injured. The specific negligent acts and  
14 omissions committed by NEG include, but are not limited to:  
15

- 16 a. Failing to adopt, implement, and maintain adequate security measures to  
17 safeguard Class Members' Private Information;
- 18 b. Failing to comply with—and thus violating—FTC Act and its regulations;
- 19 c. Failing to comply with—and thus violating—the Arizona Data Breach  
20 Notification Act and its regulations;
- 21 d. Failing to adequately monitor the security of its networks and systems;
- 22 e. Failing to ensure that its email system had plans in place to maintain  
23 reasonable data security safeguards;
- 24 f. Failing to have in place mitigation policies and procedures;
- 25 g. Allowing unauthorized access to Class Members' Private Information;
- 26  
27  
28

- 1 h. Failing to detect in a timely manner that Class Members' Private
- 2 Information had been compromised; and
- 3
- 4 i. Failing to timely notify Class Members about the Data Breach so that they
- 5 could take appropriate steps to mitigate the potential for identity theft and
- 6 other damages.

7 140. It was foreseeable that NEG's failure to use reasonable measures to protect  
8 Class Members' Private Information would result in injury to Class Members.  
9  
10 Furthermore, the breach of security was reasonably foreseeable given the known high  
11 frequency of cyberattacks and data breaches. It was therefore foreseeable that the failure  
12 to adequately safeguard Class Members' Private Information would result in one or more  
13 types of injuries to Class Members.

14  
15 141. Simply put, NEG's negligence actually and proximately caused Plaintiff and  
16 Class Members' actual, tangible, injuries-in-fact, and damages. These injuries include, but  
17 are not limited to, the theft of their Private Information by criminals, improper disclosure  
18 of their Private Information, lost value of their Private Information, and lost time and  
19 money incurred to mitigate and remediate the effects of the Data Breach that resulted from  
20 and were caused by NEG's negligence. Moreover, injuries-in-fact and damages are  
21 ongoing, imminent, and immediate.

22  
23 142. Plaintiff and Class Members are entitled to compensatory and consequential  
24 damages suffered because of the Data Breach.

25  
26 143. Plaintiff and Class Members are also entitled to injunctive relief requiring  
27 NEG to, *e.g.*, (1) strengthen its data security systems and monitoring procedures; (2)  
28

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

3  
4 **SECOND CAUSE OF ACTION**  
5 **Breach of Implied Contract**  
6 **(On behalf of the Plaintiff and the Class)**

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

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

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

16  
17 147. Plaintiff and Class Members conferred a monetary benefit on Defendant in  
18 that Defendant derived revenue from their labor, a precondition of which required  
19 Plaintiffs and Class members to entrust their Private Information to Defendant. Without  
20 the labor and Private Information provided by Plaintiffs and Class members, Defendant  
21 could not derive revenue from its regular business activities. A portion of the revenue  
22 derived from the labor and Private Information of Plaintiffs and Class members was to be  
23 used to provide a reasonable level of data security and practices, and the amount of revenue  
24 to be allocated to data security is known to Defendant.

25  
26  
27 148. Alternatively, Plaintiff and Class Members paid money to Defendant in  
28 exchange for services.

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

3           150. The implied promise of confidentiality includes consideration beyond those  
4 pre-existing general duties owed under state and federal regulations. The additional  
5 consideration included implied promises to take adequate steps to comply with specific  
6 industry data security standards and FTC guidelines on data security.  
7

8           151. The implied promises include but are not limited to: (1) taking steps to  
9 ensure that any agents who are granted access to Private Information also protect the  
10 confidentiality of that data; (2) taking steps to ensure that the information that is placed in  
11 the control of its agents is restricted and limited to achieve an authorized purpose; (3)  
12 restricting access to qualified and trained agents; (4) designing and implementing  
13 appropriate retention policies to protect the information against criminal data breaches;  
14 (5) applying or requiring proper encryption; (6) multifactor authentication for access; and  
15 (7) other steps to protect against foreseeable data breaches.  
16  
17

18           152. Based on the implicit understanding, Plaintiff and Class Members accepted  
19 NEG’s offers and provided NEG with their Private Information.  
20

21           153. Plaintiff and Class Members would not have permitted their Private  
22 Information to be collected and stored by NEG had they known that NEG would not  
23 safeguard their Private Information, as promised, or provide timely notice of a data breach.  
24

25           154. Plaintiff and Class Members fully performed their obligations under their  
26 implied contracts with NEG.  
27  
28

1 155. NEG breached the implied contracts by failing to safeguard Plaintiff’s and  
2 Class Members’ Private Information and by failing to provide them with timely and  
3 accurate notice of the Data Breach.  
4

5 156. The losses and damages Plaintiff and Class Members sustained (as described  
6 above) were the direct and proximate result of NEG’s breach of its implied contracts with  
7 Plaintiff and Class members.  
8

9 **THIRD CAUSE OF ACTION**  
10 **Unjust Enrichment**  
11 **(On Behalf of Plaintiff and the Class)**

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

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

16 159. Plaintiff and Class Members conferred a benefit on NEG, by either paying  
17 money to NEG for services or providing NEG with their labor for employment that  
18 allowed NEG to receive revenue and profits. A portion of which was intended to have  
19 been used by NEG for data security measures to secure Plaintiff and Class Members’  
20 Private Information. Plaintiff and Class Members further conferred a benefit on NEG by  
21 entrusting their Private Information to it and from which NEG derived profits.  
22

23 160. NEG enriched itself by saving the costs it reasonably should have expended  
24 on data security measures to secure Plaintiff and Class Members’ Private Information.  
25 Instead of providing a reasonable level of security that would have prevented the Data  
26 Breach, NEG chose to avoid its data security obligations at the expense of Plaintiff and  
27 Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class  
28

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

3  
4 161. Under the principles of equity and good conscience, NEG should not be  
5 permitted to retain the money belonging to Plaintiff and Class Members, because NEG  
6 failed to implement appropriate data management and security measures that are mandated  
7 by industry standards.

8  
9 162. NEG acquired the monetary benefit, PII, and PHI through inequitable means  
10 in that it failed to disclose the inadequate security practices previously alleged and failed  
11 to maintain adequate data security.

12  
13 163. If Plaintiff and Class Members knew that NEG had not secured their Private  
14 Information, they would not have agreed to give their money—or disclose their data—to  
15 NEG.

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

17  
18 165. As a direct and proximate result of NEG’s conduct, Plaintiff and Class  
19 Members have suffered—and will continue to suffer—a host of injuries, including but not  
20 limited to: (1) actual identity theft; (2) the loss of the opportunity to determine how their  
21 Private Information is used; (3) the compromise, publication, and/or theft of their Private  
22 Information; (4) out-of-pocket expenses associated with the prevention, detection, and  
23 recovery from identity theft, and/or unauthorized use of their Private Information; (5) lost  
24 opportunity costs associated with effort expended and the loss of productivity addressing  
25 and attempting to mitigate the actual and future consequences of the Data Breach,  
26 including but not limited to efforts spent researching how to prevent, detect, contest, and  
27 recover from identity theft; (6) the continued risk to their Private Information, which  
28



1 remain in NEG’s possession and are subject to further unauthorized disclosures so long as  
2 NEG fails to undertake appropriate and adequate measures to protect the Private  
3 Information in its possession; and (7) future expenditures of time, effort, and money that  
4 will be spent trying to prevent, detect, contest, and repair the impact of NEG’s Data  
5 Breach.  
6

7 166. As a direct and proximate result of NEG’s conduct, Plaintiff and Class  
8 Members suffered—and will continue to suffer—other forms of injury and/or harm.  
9

10 167. NEG should be compelled to disgorge into a common fund or constructive  
11 trust, for the benefit of Plaintiff and Class Members, proceeds that it unjustly received  
12 from Plaintiff and Class Members. Alternatively, NEG should be compelled to refund the  
13 amounts that Plaintiff and Class Members overpaid for NEG’s services.  
14

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

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

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

22 170. NEG sold Plaintiff and Class Members “merchandise” as defined by A.R.S.  
23 § 44-1521, in the form of services in connection with the properties NEG managed.

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

25 The act, use or employment by any person of any deception, deceptive or  
26 unfair act or practice, fraud, false pretense, false promise, misrepresentation,  
27 or concealment, suppression or omission of any material fact with intent that  
28 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.

1 A.R.S. § 44-1522(A).

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

5  
6 173. NEG omitted and concealed material facts, which it knew about and had the  
7 duty to disclose—namely, NEG’s inadequate privacy and security protections for  
8 Plaintiff’s and Class Members’ Private Information. This omission was designed to  
9 mislead consumers.

10  
11 174. NEG omitted and concealed those material facts even though in equity and  
12 good conscience those facts should have been disclosed and did so with the intent that  
13 others would rely on the omission, suppression, and concealment.

14  
15 175. Upon information and belief, NEG intentionally omitted and concealed  
16 material facts—like NEG’s inadequate cyber and data privacy and security protections—  
17 with the intention that consumers rely on those omissions.

18  
19 176. The concealed facts are material in that they are logically related to the  
20 transactions at issue and rationally significant to the parties in view of the nature and  
21 circumstances of those transactions.

22  
23 177. Plaintiff and Class Members were ignorant of the truth and relied on the  
24 concealed facts in providing Private Information to NEG and incurred damages as a  
25 consequent and proximate result.

26  
27 178. But for NEG’s omissions, the damage to Plaintiff and Class Members would  
28 not have occurred.

1 179. Plaintiff do not allege any claims based on any affirmative  
2 misrepresentations by NEG. Rather, Plaintiff allege that NEG omitted, failed to disclose,  
3 and concealed material facts and information as alleged herein—despite its duty to  
4 disclose such facts and information.  
5

6 180. NEG knew or should have known that its computer system and data security  
7 practices were inadequate to safeguard Plaintiff’s and Class Members’ Private  
8 Information, and that the risk of a data breach or theft was highly likely. NEG’s actions in  
9 engaging in these deceptive acts and practices were intentional, knowing, willful, wanton,  
10 and reckless with respect to the rights of Plaintiff and Class Members.  
11

12 181. Specifically, NEG failed to comply with the standards outlined by the FTC  
13 Act. NEG was or should have been aware of these standards. NEG’s data security systems  
14 did not follow the FTC’s guidelines. And thus, NEG’s systems operated below the  
15 minimum standards required.  
16

17 182. Plaintiff and Class Members were ignorant of the truth and relied on the  
18 concealed facts in providing their Private Information and incurred damages as a  
19 consequent and proximate result.  
20

21 183. Plaintiff and Class Members seek all available relief under A.R.S. §§ 44-  
22 1521, *et seq.*, including, but not limited to, compensatory damages, punitive damages,  
23 injunctive relief, and attorneys’ fees and costs.  
24

25 **PRAYER FOR RELIEF**

26 WHEREFORE Plaintiff, on behalf of themselves and all others similarly situated,  
27 request the following relief:  
28

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

- 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;

- 1           vi. prohibiting NEG from maintaining Plaintiff's and Class Members'  
2           Private Information on a cloud-based database;
- 3           vii. requiring NEG to segment data by creating firewalls and access  
4           controls so that, if one area of NEG's network is compromised,  
5           hackers cannot gain access to other portions of NEG's systems;
- 6           viii. requiring NEG to conduct regular database scanning and securing  
7           checks;
- 8           ix. requiring NEG to monitor ingress and egress of all network traffic;
- 9           x. requiring NEG to establish an information security training program  
10           that includes at least annual information security training for all  
11           employees, with additional training to be provided as appropriate  
12           based upon the employees' respective responsibilities with handling  
13           Private Information, as well as protecting the Private Information of  
14           Plaintiff and Class Members;
- 15           xi. requiring NEG to implement a system of tests to assess its respective  
16           employees' knowledge of the education programs discussed in  
17           the preceding subparagraphs, as well as randomly and periodically  
18           testing employees' compliance with NEG's policies, programs, and  
19           systems for protecting personal identifying information;
- 20           xii. requiring NEG to implement, maintain, review, and revise as  
21           necessary a threat management program to appropriately monitor  
22           NEG's networks for internal and external threats, and assess whether  
23           monitoring tools are properly configured, tested, and updated;
- 24  
25  
26  
27  
28

- 1           xiii.    requiring NEG to meaningfully educate all Class Members about the
- 2                    threats that they face because of the loss of its confidential personal
- 3                    identifying information to third parties, as well as the steps
- 4                    affected individuals must take to protect themselves; and
- 5
- 6           xiv.    requiring NEG to provide adequate credit monitoring to all Class
- 7                    Members.
- 8

- 9           C.    A mandatory injunction requiring that NEG provide notice to each member
- 10                   of the Class relating to the full nature and extent of the Data Breach and the
- 11                   disclosure of Private Information to unauthorized persons;
- 12           D.    Enjoining NEG from further deceptive practices and making untrue
- 13                   statements about the Data Breach and the stolen Private Information;
- 14           E.    An award of damages, including actual, nominal, consequential damages, and
- 15                   punitive, as allowed by law in an amount to be determined;
- 16           F.    An award of attorneys’ fees, costs, and litigation expenses, as allowed by law;
- 17           G.    An award of pre- and post-judgment interest, costs, attorneys’ fees, expenses,
- 18                   and interest as permitted by law;
- 19           H.    Granting the Plaintiff and the Class leave to amend this complaint to conform
- 20                   to the evidence produced at trial;
- 21           I.    For all other Orders, findings, and determinations identified and sought in this
- 22                   Complaint; and
- 23           J.    Such other and further relief as this court may deem just and proper.
- 24
- 25
- 26
- 27
- 28

**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***

# ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [New Enchantment Group Hit with Class Action Over October 2022 Data Breach](#)

---