

John J. Nelson (SBN 317598)  
**MILBERG COLEMAN BRYSON  
PHILLIPS GROSSMAN, PLLC**  
280 S. Beverly Drive  
Beverly Hills, CA 90212  
Telephone: (858) 209-6941  
Email: jnelson@milberg.com

*Attorney for Plaintiff and the Proposed Class*

**IN THE UNITED STATES DISTRICT COURT  
FOR THE CENTRAL DISTRICT OF CALIFORNIA**

Laura Wielkopolski, individually and  
on behalf of all others similarly  
situated,

Plaintiff,

v.

Form I-9 Compliance, LLC,

Defendant.

Case No. \_\_\_\_\_

**CLASS ACTION COMPLAINT**

**DEMAND FOR JURY TRIAL**

Plaintiff Laura Wilcopolski (“Plaintiff”) brings this Class Action Complaint (“Complaint”) against Defendant Form I-9 Compliance, LLC (“Defendant” or “FIC”) as an individual and on behalf of all others similarly situated, and alleges, upon personal knowledge as to her own actions and her counsels’ investigation, and upon information and belief as to all other matters, as follows:

## NATURE OF THE ACTION

1  
2 1. This class action arises out of the recent data breach (“Data Breach”)  
3  
4 involving Defendant, a limited liability company that assists its clients in completing  
5 the government required Form I-9 documents in connection with its clients’  
6 employees employment.

7  
8 2. Plaintiff brings this Complaint against Defendant for its failure to  
9 properly secure and safeguard the personally identifiable information that it  
10 collected and maintained as part of its regular business practices, including  
11 Plaintiff’s and Class Members’ names, dates of birth, addresses, hire dates, and  
12 Social Security numbers, (collectively defined herein as “PII”).  
13

14 3. Upon information and belief, current and former employees at  
15 Defendant’s clients are required to entrust Defendant with sensitive, non-public PII,  
16 without which Defendant could not perform its regular business activities, in order  
17 to obtain employment or certain employment benefits at Defendant’s clients.  
18 Defendant retains this information for at least many years and even after the  
19 employee-employer relationship has ended.  
20

21 4. By obtaining, collecting, using, and deriving a benefit from the PII of  
22 Plaintiff and Class Members, Defendant assumed legal and equitable duties to those  
23 individuals to protect and safeguard that information from unauthorized access and  
24 intrusion.  
25  
26  
27  
28

1           5. Defendant's investigation concluded that the PII compromised in the  
2 Data Breach included Plaintiff's and approximately 27,000 other individuals'  
3 information.<sup>1</sup>  
4

5           6. Defendant failed to adequately protect Plaintiff's and Class Members  
6 PII—and failed to even encrypt or redact this highly sensitive information. This  
7 unencrypted, unredacted PII was compromised due to Defendant's negligent and/or  
8 careless acts and omissions and its utter failure to protect employees' sensitive data.  
9 Hackers targeted and obtained Plaintiff's and Class Members' PII because of its  
10 value in exploiting and stealing the identities of Plaintiff and Class Members. The  
11 present and continuing risk of identity theft and fraud to victims of the Data Breach  
12 will remain for their respective lifetimes.  
13  
14  
15

16           7. In breaching its duties to properly safeguard its clients' employees' PII  
17 and give employees timely, adequate notice of the Data Breach's occurrence,  
18 Defendant's conduct amounts to negligence and/or recklessness and violates federal  
19 and state statutes.  
20

21           8. Plaintiff brings this action on behalf of all persons whose PII was  
22 compromised as a result of Defendant's failure to: (i) adequately protect the PII of  
23 Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of Defendant's  
24  
25  
26

---

27 <sup>1</sup> [https://apps.web.maine.gov/online/aeviewer/ME/40/c0ea4ec7-a813-433b-b966-](https://apps.web.maine.gov/online/aeviewer/ME/40/c0ea4ec7-a813-433b-b966-e1201d2b92ca.shtml)  
28 [e1201d2b92ca.shtml](https://apps.web.maine.gov/online/aeviewer/ME/40/c0ea4ec7-a813-433b-b966-e1201d2b92ca.shtml)

1 inadequate information security practices; and (iii) effectively secure hardware  
2 containing protected PII using reasonable and effective security procedures free of  
3 vulnerabilities and incidents. Defendant's conduct amounts at least to negligence  
4 and violates federal and state statutes.  
5

6         9. Defendant disregarded the rights of Plaintiff and Class Members by  
7 intentionally, willfully, recklessly, or negligently failing to implement and maintain  
8 adequate and reasonable measures to ensure that the PII of Plaintiff and Class  
9 Members was safeguarded, failing to take available steps to prevent an unauthorized  
10 disclosure of data, and failing to follow applicable, required, and appropriate  
11 protocols, policies, and procedures regarding the encryption of data, even for internal  
12 use. As a result, the PII of Plaintiff and Class Members was compromised through  
13 disclosure to an unknown and unauthorized third party. Plaintiff and Class Members  
14 have a continuing interest in ensuring that their information is and remains safe, and  
15 they should be entitled to injunctive and other equitable relief.  
16  
17  
18  
19

20         10. Plaintiff and Class Members have suffered injury as a result of  
21 Defendant's conduct. These injuries include: (i) invasion of privacy; (ii) theft of their  
22 PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs  
23 associated with attempting to mitigate the actual consequences of the Data Breach;  
24 (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with  
25 attempting to mitigate the actual consequences of the Data Breach; (vii) actual  
26  
27  
28

1 misuse of the compromised data consisting of an increase in spam calls, texts, and/or  
2 emails; (viii) nominal damages; and (ix) the continued and certainly increased risk  
3 to their PII, which: (a) remains unencrypted and available for unauthorized third  
4 parties to access and abuse; and (b) remains backed up in Defendant's possession  
5 and is subject to further unauthorized disclosures so long as Defendant fails to  
6 undertake appropriate and adequate measures to protect the PII.  
7  
8

9 11. Plaintiff seeks to remedy these harms and prevent any future data  
10 compromise on behalf of herself and all similarly situated persons whose personal  
11 data was compromised and stolen as a result of the Data Breach and who remain at  
12 risk due to Defendant's inadequate data security practices.  
13

## 14 **PARTIES**

15  
16 12. Plaintiff Laura Wilcopolski is a natural resident and citizen of Lockport,  
17 Illinois.  
18

19 13. Defendant is a limited liability company organized under the state laws  
20 of California with its principal place of business located in Newport Beach,  
21 California.  
22

## 23 **JURISDICTION AND VENUE**

24 14. This Court has subject matter jurisdiction over this action under 28  
25 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy  
26 exceeds the sum or value of \$5,000,000, exclusive of interest and costs, there are  
27  
28

1 more than 100 members in the proposed class, and at least one member of the class,  
2 including Plaintiff, is a citizen of a state different from Defendant.

3  
4 15. This Court has personal jurisdiction over Defendant because its  
5 principal place of business is in this District, regularly conducts business in  
6 Pennsylvania, and the acts and omissions giving rise to Plaintiff's claims occurred in  
7 and emanated from this District.  
8

9 16. Venue is proper under 18 U.S.C § 1391(b)(1) because Defendant's  
10 principal place of business is in this District.  
11

## 12 **FACTUAL ALLEGATIONS**

### 13 ***Background of Defendant.***

14 17. Defendant is a limited liability company that assists its clients in  
15 completing the government required Form I-9 documents in connection with its  
16 clients' employees' employment.  
17

18 18. Plaintiff and Class Members are current and former employees of  
19 Defendant's clients.  
20

21 19. In order to apply to be an employee or obtain certain employment-  
22 related benefits at Defendant's clients, Plaintiff and Class Members were required  
23 to provide sensitive and confidential PII, including their names, dates of birth,  
24 addresses, and Social Security numbers.  
25  
26  
27  
28

1        20. The information held by Defendant in its computer systems at the time  
2 of the Data Breach included the unencrypted PII of Plaintiff and Class Members.

3  
4        21. Upon information and belief, Defendant made promises and  
5 representations to its clients' employees, including Plaintiff and Class Members, that  
6 the PII collected from them as a condition of their employment would be kept safe,  
7 confidential, that the privacy of that information would be maintained, and that  
8 Defendant would delete any sensitive information after it was no longer required to  
9 maintain it.  
10

11  
12        22. Indeed, Defendant provides on its website that: "Form I-9 Compliance  
13 secures your personal information from unauthorized access, use or disclosure. Data  
14 collected by Form I-9 Compliance is protected by multiple hardware and software  
15 layers that allow secure web interactions and business-to-business communication  
16 without compromise. High level security design that includes TLS 1.2, multiple fire  
17 walls, access protocols, physical security, and several levels of anti-spam and anti-  
18 virus protection ensure data security. In addition, Form I-9 Compliance does not  
19 compile information into a database for resale."<sup>2</sup>  
20  
21

22        23. Plaintiff and Class Members provided their PII to Defendant with the  
23 reasonable expectation and on the mutual understanding that Defendant would  
24  
25  
26

---

27 <sup>2</sup> <https://www.formi9.com/resources/privacy-policy/>  
28

1 comply with its obligations to keep such information confidential and secure from  
2 unauthorized access.

3  
4 24. Plaintiff and Class Members have taken reasonable steps to maintain  
5 the confidentiality of their PII. Plaintiff and Class Members relied on the  
6 sophistication of Defendant to keep their PII confidential and securely maintained,  
7 to use this information for necessary purposes only, and to make only authorized  
8 disclosures of this information. Plaintiff and Class Members value the  
9 confidentiality of their PII and demand security to safeguard their PII.  
10

11  
12 25. Defendant had a duty to adopt reasonable measures to protect the PII of  
13 Plaintiff and Class Members from involuntary disclosure to third parties. Defendant  
14 has a legal duty to keep its clients' employees' PII safe and confidential.  
15

16 26. Defendant had obligations created by FTC Act, contract, industry  
17 standards, and representations made to Plaintiff and Class Members, to keep their  
18 PII confidential and to protect it from unauthorized access and disclosure.  
19

20 27. Defendant derived a substantial economic benefit from collecting  
21 Plaintiff's and Class Members' PII. Without the required submission of PII,  
22 Defendant could not perform the services it provides.  
23

24 28. By obtaining, collecting, using, and deriving a benefit from Plaintiff's  
25 and Class Members' PII, Defendant assumed legal and equitable duties and knew or  
26  
27  
28



1 should have known that it was responsible for protecting Plaintiff's and Class  
2 Members' PII from disclosure.

3  
4 ***The Data Breach.***

5 29. On or about May 31, 2024, Defendant began sending Plaintiff and other  
6 victims of the Data Breach a Notice of Security Incident letter (the "Notice Letter"),  
7 informing them that:  
8

9 **What Happened?**

10 On or about February 5, 2024, an unauthorized third party obtained access to  
11 a portion of Form I-9's network. On April 12, 2024, we became aware of the  
12 unauthorized activity and promptly took a portion of our network offline,  
13 activated our response process, and launched an investigation of the incident  
14 with the support of external cybersecurity experts. We also reported the  
incident to law enforcement.

15 **What Information Was Involved?**

16 Our investigation determined that some of your personal information was  
17 affected by this incident. This information included your name, address,  
18 Social Security number, date of birth, and hire date.<sup>3</sup>

19 30. Omitted from the Notice Letter were the identity of the cybercriminals  
20 who perpetrated this Data Breach, the details of the root cause of the Data Breach,  
21 the vulnerabilities exploited, and the remedial measures undertaken to ensure such a  
22 breach does not occur again. To date, these critical facts have not been explained or  
23  
24  
25

---

26 <sup>3</sup> The "Notice Letter". A sample copy is available at  
27 [https://apps.web.maine.gov/online/aevviewer/ME/40/c0ea4ec7-a813-433b-b966-](https://apps.web.maine.gov/online/aevviewer/ME/40/c0ea4ec7-a813-433b-b966-e1201d2b92ca.shtml)  
28 [e1201d2b92ca.shtml](https://apps.web.maine.gov/online/aevviewer/ME/40/c0ea4ec7-a813-433b-b966-e1201d2b92ca.shtml)

1 clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that  
2 their PII remains protected.

3  
4 31. This “disclosure” amounts to no real disclosure at all, as it fails to  
5 inform, with any degree of specificity, Plaintiff and Class Members of the Data  
6 Breach’s critical facts. Without these details, Plaintiff’s and Class Members’ ability  
7 to mitigate the harms resulting from the Data Breach is severely diminished.  
8

9 32. Despite Defendant’s intentional opacity about the root cause of this  
10 incident, several facts may be gleaned from the Notice Letter, including: a) that this  
11 Data Breach was the work of cybercriminals; b) that the cybercriminals first  
12 infiltrated Defendant’s networks and systems, and downloaded data from the  
13 networks and systems (aka exfiltrated data, or in layperson’s terms “stole” data; and  
14 c) that once inside Defendant’s networks and systems, the cybercriminals targeted  
15 information including Plaintiff’s and Class Members’ Social Security numbers and  
16 other sensitive information for download and theft.  
17  
18

19  
20 33. Moreover, in its Notice Letter, Defendant failed to specify whether it  
21 undertook any efforts to contact the approximate 27,000 Class Members whose data  
22 was accessed and acquired in the Data Breach to inquire whether any of the Class  
23 Members suffered misuse of their data, whether Class Members should report their  
24 misuse to Defendant, and whether Defendant set up any mechanism for Class  
25 Members to report any misuse of their data.  
26  
27  
28

1       34. Defendant did not use reasonable security procedures and practices  
2 appropriate to the nature of the sensitive information they were maintaining for  
3 Plaintiff and Class Members, causing the exposure of PII, such as encrypting the  
4 information or deleting it when it is no longer needed.  
5

6       35. The attacker targeted, accessed, and acquired files in Defendant's  
7 computer systems containing unencrypted PII of Plaintiff and Class Members,  
8 including their names, dates of birth, addresses, and Social Security numbers.  
9 Plaintiff's and Class Members' PII was accessed and stolen in the Data Breach.  
10

11       36. Plaintiff further believes that her PII and that of Class Members, was  
12 subsequently sold on the dark web following the Data Breach, as that is the *modus*  
13 *operandi* of cybercriminals that commit cyber-attacks of this type.  
14

15       ***Data Breaches Are Preventable.***  
16

17       37. Defendant could have prevented this Data Breach by, among other  
18 things, properly encrypting or otherwise protecting their equipment and computer  
19 files containing PII.  
20

21       38. As explained by the Federal Bureau of Investigation, "[p]revention is  
22 the most effective defense against ransomware and it is critical to take precautions  
23 for protection."<sup>4</sup>  
24

25  
26  
27       <sup>4</sup> How to Protect Your Networks from RANSOMWARE, at 3, available at:  
28 <https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view>

1           39. To prevent and detect cyber-attacks, Defendant could and should have  
2 implemented, as recommended by the United States Government, the following  
3 measures:  
4

- 5           ● Implement an awareness and training program. Because end users are  
6 targets, employees and individuals should be aware of the threat of  
7 ransomware and how it is delivered.
- 8           ● Enable strong spam filters to prevent phishing emails from reaching the end  
9 users and authenticate inbound email using technologies like Sender Policy  
10 Framework (SPF), Domain Message Authentication Reporting and  
11 Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to  
12 prevent email spoofing.
- 13           ● Scan all incoming and outgoing emails to detect threats and filter  
14 executable files from reaching end users.
- 15           ● Configure firewalls to block access to known malicious IP addresses.
- 16           ● Patch operating systems, software, and firmware on devices. Consider  
17 using a centralized patch management system.
- 18           ● Set anti-virus and anti-malware programs to conduct regular scans  
19 automatically.
- 20           ● Manage the use of privileged accounts based on the principle of least  
21 privilege: no users should be assigned administrative access unless  
22 absolutely needed; and those with a need for administrator accounts should  
23 only use them when necessary.
- 24           ● Configure access controls—including file, directory, and network share  
25 permissions—with least privilege in mind. If a user only needs to read  
26 specific files, the user should not have write access to those files,  
27 directories, or shares.
- 28           ● Disable macro scripts from office files transmitted via email. Consider  
using Office Viewer software to open Microsoft Office files transmitted via  
email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.<sup>5</sup>

40. To prevent and detect cyber-attacks or ransomware attacks, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

**Secure internet-facing assets**

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

**Thoroughly investigate and remediate alerts**

- Prioritize and treat commodity malware infections as potential full compromise;

**Include IT Pros in security discussions**

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

---

<sup>5</sup> *Id.* at 3-4.

1       **Build credential hygiene**

- 2       -       Use [multifactor authentication] or [network level authentication] and  
3       use strong, randomized, just-in-time local admin passwords;

4       **Apply principle of least-privilege**

- 5  
6       -       Monitor for adversarial activities  
7       -       Hunt for brute force attempts  
8       -       Monitor for cleanup of Event Logs  
9       -       Analyze logon events;

10       **Harden infrastructure**

- 11       -       Use Windows Defender Firewall  
12       -       Enable tamper protection  
13       -       Enable cloud-delivered protection  
14       -       Turn on attack surface reduction rules and [Antimalware Scan  
15       Interface] for Office [Visual Basic for Applications].<sup>6</sup>

16       41.    Given that Defendant were storing the sensitive PII of its clients'  
17   current and former employees, Defendant could and should have implemented all of  
18   the above measures to prevent and detect cyberattacks.

19       42.    The occurrence of the Data Breach indicates that Defendant failed to  
20   adequately implement one or more of the above measures to prevent cyberattacks,  
21   resulting in the Data Breach and the exposure of the PII of approximately 27,000  
22   employees, including that of Plaintiff and Class Members.  
23

24  
25  
26       <sup>6</sup> See Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at*:  
27   [https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-](https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/)  
28   preventable-disaster/ (last visited Nov. 11, 2021).

***Defendant Acquires, Collects, and Stores Its Clients' Employees' PII***

43. As a condition of employment with Defendant's clients, Plaintiff and Class Members were required to give their sensitive and confidential PII to Defendant.

44. Defendant retains and stores this information and derives a substantial economic benefit from the PII that it collects. But for the collection of Plaintiff's and Class Members' PII, Defendant would be unable to perform its services.

45. By obtaining, collecting, and storing the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known that they were responsible for protecting the PII from disclosure.

46. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and relied on Defendant to keep their PII confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

47. Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the PII of Plaintiff and Class Members.

***Defendant Knew or Should Have Known of the Risk Because Compliance Companies in Possession of PII are Particularly Susceptible to Cyber Attacks.***

48. Data thieves regularly target companies like Defendant's due to the highly sensitive information that they custody. Defendant knew and understood that unprotected PII is valuable and highly sought after by criminal parties who seek to illegally monetize that PII through unauthorized access.

49. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting compliance companies that collect and store PII and other sensitive information, like Defendant, preceding the date of the breach.

50. According to the *2023 Annual Data Breach Report*, the number of data compromises in 2023 (3,205) increased by 78 percentage points compared to 2022 (1,801).<sup>7</sup> The ITRC set a new record for the number of data compromises tracked in a year, up 72 percentage points from the previous all-time high in 2021 (1,860).<sup>8</sup>

51. In light of recent high profile data breaches at other industry leading companies, including T-Mobile, USA (37 million records, February-March 2023), 23andMe, Inc. (20 million records, October 2023), Wilton Reassurance Company (1.4 million records, June 2023), NCB Management Services, Inc. (1 million

---

<sup>7</sup> <https://www.idtheftcenter.org/publication/2023-data-breach-report/>

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



1 records, February 2023), Defendant knew or should have known that the PII that it  
2 collected and maintained would be targeted by cybercriminals.

3  
4 52. Additionally, as companies became more dependent on computer  
5 systems to run their business,<sup>9</sup> *e.g.*, working remotely as a result of the Covid-19  
6 pandemic, and the Internet of Things (“IoT”), the danger posed by cybercriminals is  
7 magnified, thereby highlighting the need for adequate administrative, physical, and  
8 technical safeguards.<sup>10</sup>

9  
10 53. As a custodian of PII, Defendant knew, or should have known, the  
11 importance of safeguarding the PII entrusted to it by Plaintiff and Class members,  
12 and of the foreseeable consequences if its data security systems were breached,  
13 including the significant costs imposed on Plaintiff and Class Members as a result  
14 of a breach.  
15

16  
17 54. Despite the prevalence of public announcements of data breach and  
18 data security compromises, Defendant failed to take appropriate steps to protect the  
19 PII of Plaintiff and Class Members from being compromised.  
20

21 55. At all relevant times, Defendant knew, or reasonably should have  
22 known, of the importance of safeguarding the PII of Plaintiff and Class Members  
23 and of the foreseeable consequences that would occur if Defendant's data security  
24

25  
26 <sup>9</sup> <https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html>

27 <sup>10</sup> <https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022>  
28

1 system was breached, including, specifically, the significant costs that would be  
2 imposed on Plaintiff and Class Members as a result of a breach.

3  
4 56. Defendant was, or should have been, fully aware of the unique type and  
5 the significant volume of data on Defendant's server(s), amounting to more than  
6 twenty thousand individuals' detailed, PII, and, thus, the significant number of  
7 individuals who would be harmed by the exposure of the unencrypted data.  
8

9 57. In the Notice Letter, Defendant makes an offer of 24 months of identity  
10 monitoring services. This is wholly inadequate to compensate Plaintiff and Class  
11 Members as it fails to provide for the fact victims of data breaches and other  
12 unauthorized disclosures commonly face multiple years of ongoing identity theft,  
13 financial fraud, and it entirely fails to provide sufficient compensation for the  
14 unauthorized release and disclosure of Plaintiff and Class Members' PII. Moreover,  
15 once this service expires, Plaintiff and Class Members will be forced to pay out of  
16 pocket for necessary identity monitoring services.  
17  
18  
19

20 58. Defendant's offering of credit and identity monitoring establishes that  
21 Plaintiff and Class Members' sensitive PII *was* in fact affected, accessed,  
22 compromised, and exfiltrated from Defendant's computer systems.  
23

24 59. The injuries to Plaintiff and Class Members were directly and  
25 proximately caused by Defendant's failure to implement or maintain adequate data  
26 security measures for the PII of Plaintiff and Class Members.  
27  
28

1           60. The ramifications of Defendant's failure to keep secure the PII of  
2 Plaintiff and Class Members are long lasting and severe. Once PII is stolen—  
3 particularly Social Security numbers—fraudulent use of that information and  
4 damage to victims may continue for years.

5  
6           61. As a compliance company in possession of its clients' employees' and  
7 former employees' PII, Defendant knew, or should have known, the importance of  
8 safeguarding the PII entrusted to them by Plaintiff and Class Members and of the  
9 foreseeable consequences if its data security systems were breached. This includes  
10 the significant costs imposed on Plaintiff and Class Members as a result of a breach.  
11  
12 Nevertheless, Defendant failed to take adequate cybersecurity measures to prevent  
13 the Data Breach.  
14

15  
16           ***Value of Personally Identifying Information.***

17           62. The Federal Trade Commission ("FTC") defines identity theft as "a  
18 fraud committed or attempted using the identifying information of another person  
19 without authority."<sup>11</sup> The FTC describes "identifying information" as "any name or  
20 number that may be used, alone or in conjunction with any other information, to  
21 identify a specific person," including, among other things, "[n]ame, Social Security  
22 number, date of birth, official State or government issued driver's license or  
23  
24  
25  
26

27  
28  

---

<sup>11</sup> 17 C.F.R. § 248.201 (2013).

1 identification number, alien registration number, government passport number,  
 2 employer or taxpayer identification number.”<sup>12</sup>

3  
 4 63. The PII of individuals remains of high value to criminals, as evidenced  
 5 by the prices they will pay through the dark web. Numerous sources cite dark web  
 6 pricing for stolen identity credentials.<sup>13</sup> For example, Personal Information can be  
 7 sold at a price ranging from \$40 to \$200.<sup>14</sup> Criminals can also purchase access to  
 8 entire company data breaches from \$900 to \$4,500.<sup>15</sup>

9  
 10 64. Moreover, Social Security numbers are among the worst kind of PII to  
 11 have stolen because they may be put to a variety of fraudulent uses and are difficult  
 12 for an individual to change.

13  
 14 65. According to the Social Security Administration, each time an  
 15 individual’s Social Security number is compromised, “the potential for a thief to  
 16 illegitimately gain access to bank accounts, credit cards, driving records, tax and  
 17 employment histories and other private information increases.”<sup>16</sup> Moreover,  
 18  
 19  
 20

21 <sup>12</sup> *Id.*

22 <sup>13</sup> *Your personal data is for sale on the dark web. Here’s how much it costs*, Digital Trends, Oct.  
 23 16, 2019, available at: [https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-](https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/)  
 24 [web-how-much-it-costs/](https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/) (last visited Oct. 17, 2022).

25 <sup>14</sup> *Here’s How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6,  
 26 2017, available at: [https://www.experian.com/blogs/ask-experian/heres-how-much-your-](https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/)  
 27 [personal-information-is-selling-for-on-the-dark-web/](https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/) (last visited Oct. 17, 2022).

28 <sup>15</sup> *In the Dark*, VPNOOverview, 2019, available at: [https://vpnooverview.com/privacy/anonymous-](https://vpnooverview.com/privacy/anonymous-browsing/in-the-dark/)  
[browsing/in-the-dark/](https://vpnooverview.com/privacy/anonymous-browsing/in-the-dark/) (last visited Oct. 21, 2022).

<sup>16</sup> See <https://www.ssa.gov/phila/ProtectingSSNs.htm#:~:text=An%20organization's%20collection%20and%20use,and%20other%20private%20information%20increases.>

1 “[b]ecause many organizations still use SSNs as the primary identifier, exposure to  
2 identity theft and fraud remains.”<sup>17</sup>

3  
4 66. The Social Security Administration stresses that the loss of an  
5 individual’s Social Security number, as experienced by Plaintiff and some Class  
6 Members, can lead to identity theft and extensive financial fraud:

7  
8 A dishonest person who has your Social Security number can use it to get  
9 other personal information about you. Identity thieves can use your number  
10 and your good credit to apply for more credit in your name. Then, they use  
11 the credit cards and don’t pay the bills, it damages your credit. You may not  
12 find out that someone is using your number until you’re turned down for  
13 credit, or you begin to get calls from unknown creditors demanding payment  
14 for items you never bought. Someone illegally using your Social Security  
15 number and assuming your identity can cause a lot of problems.<sup>18</sup>

16  
17 67. In fact, “[a] stolen Social Security number is one of the leading causes  
18 of identity theft and can threaten your financial health.”<sup>19</sup> “Someone who has your  
19 SSN can use it to impersonate you, obtain credit and open bank accounts, apply for  
20 jobs, steal your tax refunds, get medical treatment, and steal your government  
21 benefits.”<sup>20</sup>

22 68. What’s more, it is no easy task to change or cancel a stolen Social  
23 Security number. An individual cannot obtain a new Social Security number without

---

24 <sup>17</sup> *Id.*

25 <sup>18</sup> Social Security Administration, *Identity Theft and Your Social Security Number*, available at:  
<https://www.ssa.gov/pubs/EN-05-10064.pdf>

26 <sup>19</sup> See [https://www.equifax.com/personal/education/identity-theft/articles/-/learn/social-security-](https://www.equifax.com/personal/education/identity-theft/articles/-/learn/social-security-number-identity-theft/)  
27 [number-identity-theft/](https://www.equifax.com/personal/education/identity-theft/articles/-/learn/social-security-number-identity-theft/)

28 <sup>20</sup> See <https://www.investopedia.com/terms/s/ssn.asp>

1 significant paperwork and evidence of actual misuse. In other words, preventive  
2 action to defend against the possibility of misuse of a Social Security number is not  
3 permitted; an individual must show evidence of actual, ongoing fraud activity to  
4 obtain a new number.  
5

6 69. Even then, a new Social Security number may not be effective.  
7 According to Julie Ferguson of the Identity Theft Resource Center, “[t]he credit  
8 bureaus and banks are able to link the new number very quickly to the old number,  
9 so all of that old bad information is quickly inherited into the new Social Security  
10 number.”<sup>21</sup>  
11

12  
13 70. For these reasons, some courts have referred to Social Security numbers  
14 as the “gold standard” for identity theft. *Portier v. NEO Tech. Sols.*, No. 3:17-CV-  
15 30111, 2019 WL 7946103, at \*12 (D. Mass. Dec. 31, 2019) (“Because Social  
16 Security numbers are the gold standard for identity theft, their theft is significant . .  
17 . . Access to Social Security numbers causes long-lasting jeopardy because the Social  
18 Security Administration does not normally replace Social Security numbers.”),  
19 report and recommendation adopted, No. 3:17-CV-30111, 2020 WL 877035 (D.  
20 Mass. Jan. 30, 2020); *see also McFarlane v. Altice USA, Inc.*, 2021 WL 860584, at  
21 \*4 (citations omitted) (S.D.N.Y. Mar. 8, 2021) (the court noted that Plaintiff’s Social  
22  
23  
24  
25

---

26 <sup>21</sup> Bryan Naylor, *Victims of Social Security Number Theft Find It’s Hard to Bounce Back*, NPR  
27 (Feb. 9, 2015), available at: <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft>  
28

1 Security numbers are: arguably “the most dangerous type of personal information in  
2 the hands of identity thieves” because it is immutable and can be used to  
3 “impersonat[e] [the victim] to get medical services, government benefits, ... tax  
4 refunds, [and] employment.” . . . Unlike a credit card number, which can be changed  
5 to eliminate the risk of harm following a data breach, “[a] social security number  
6 derives its value in that it is immutable,” and when it is stolen it can “forever be  
7 wielded to identify [the victim] and target her in fraudulent schemes and identity  
8 theft attacks.”)

11  
12 71. Similarly, the California state government warns consumers that:  
13 “[o]riginally, your Social Security number (SSN) was a way for the government to  
14 track your earnings and pay you retirement benefits. But over the years, it has  
15 become much more than that. It is the key to a lot of your personal information. With  
16 your name and SSN, an identity thief could open new credit and bank accounts, rent  
17 an apartment, or even get a job.”<sup>22</sup>

19  
20 72. Based on the foregoing, the information compromised in the Data  
21 Breach is significantly more valuable than the loss of, for example, credit card  
22 information in a data breach because, there, victims can cancel or close credit and  
23 debit card accounts. The information compromised in this Data Breach is impossible  
24  
25  
26

---

27 <sup>22</sup> See <https://oag.ca.gov/idtheft/facts/your-ssn>  
28

1 to “close” and difficult, if not impossible, to change—Social Security number, date  
2 of birth, and name.

3  
4 73. This data demands a much higher price on the black market. Martin  
5 Walter, senior director at cybersecurity firm RedSeal, explained, “Compared to  
6 credit card information, personally identifiable information and Social Security  
7 numbers are worth more than 10x on the black market.”<sup>23</sup>  
8

9 74. Among other forms of fraud, identity thieves may obtain driver’s  
10 licenses, government benefits, medical services, and housing or even give false  
11 information to police.  
12

13 75. The fraudulent activity resulting from the Data Breach may not come  
14 to light for years. There may be a time lag between when harm occurs versus when  
15 it is discovered, and also between when PII is stolen and when it is used. According  
16 to the U.S. Government Accountability Office (“GAO”), which conducted a study  
17 regarding data breaches:  
18  
19

20 [L]aw enforcement officials told us that in some cases, stolen data may be  
21 held for up to a year or more before being used to commit identity theft.  
22 Further, once stolen data have been sold or posted on the Web, fraudulent use  
23 of that information may continue for years. As a result, studies that attempt to  
24 measure the harm resulting from data breaches cannot necessarily rule out all  
future harm.<sup>24</sup>

25 <sup>23</sup> Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card*  
26 *Numbers*, IT World, (Feb. 6, 2015), available at:  
<https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last visited Oct. 17, 2022).

27 <sup>24</sup> *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at:  
28 <https://www.gao.gov/assets/gao-07-737.pdf> (last visited Oct. 17, 2022).



1  
2 76. Plaintiff and Class Members now face years of constant surveillance of  
3 their financial and personal records, monitoring, and loss of rights. The Class is  
4 incurring and will continue to incur such damages in addition to any fraudulent use  
5 of their PII.  
6

7 ***Defendant Fails to Comply with FTC Guidelines.***

8 77. The Federal Trade Commission (“FTC”) has promulgated numerous  
9 guides for businesses which highlight the importance of implementing reasonable  
10 data security practices. According to the FTC, the need for data security should be  
11 factored into all business decision-making.  
12  
13

14 78. In 2016, the FTC updated its publication, Protecting Personal  
15 Information: A Guide for Business, which established cyber-security guidelines for  
16 businesses. These guidelines note that businesses should protect the personal  
17 employee information that they keep; properly dispose of personal information that  
18 is no longer needed; encrypt information stored on computer networks; understand  
19 their network’s vulnerabilities; and implement policies to correct any security  
20 problems.<sup>25</sup>  
21  
22  
23  
24  
25

---

26 <sup>25</sup> *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016).  
27 Available at [https://www.ftc.gov/system/files/documents/plain-language/pdf-0136\\_proteting-](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf)  
28 [personal-information.pdf](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf) (last visited Oct. 17, 2022).

1       79. The guidelines also recommend that businesses use an intrusion  
2 detection system to expose a breach as soon as it occurs; monitor all incoming traffic  
3 for activity indicating someone is attempting to hack the system; watch for large  
4 amounts of data being transmitted from the system; and have a response plan ready  
5 in the event of a breach.<sup>26</sup>  
6

7  
8       80. The FTC further recommends that companies not maintain PII longer  
9 than is needed for authorization of a transaction; limit access to sensitive data;  
10 require complex passwords to be used on networks; use industry-tested methods for  
11 security; monitor for suspicious activity on the network; and verify that third-party  
12 service providers have implemented reasonable security measures.  
13

14  
15       81. The FTC has brought enforcement actions against businesses for failing  
16 to adequately and reasonably protect employee data, treating the failure to employ  
17 reasonable and appropriate measures to protect against unauthorized access to  
18 confidential employee data as an unfair act or practice prohibited by Section 5 of the  
19 Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. Orders resulting from  
20 these actions further clarify the measures businesses must take to meet their data  
21 security obligations.  
22

23  
24       82. These FTC enforcement actions include actions against compliance  
25 companies, like Defendant.  
26

---

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

1           83. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits “unfair . . . practices  
2 in or affecting commerce,” including, as interpreted and enforced by the FTC, the  
3 unfair act or practice by businesses, such as Defendant, of failing to use reasonable  
4 measures to protect PII. The FTC publications and orders described above also form  
5 part of the basis of Defendant’s duty in this regard.  
6

7  
8           84. Defendant failed to properly implement basic data security practices.

9           85. Defendant’s failure to employ reasonable and appropriate measures to  
10 protect against unauthorized access to its clients’ employees’ PII or to comply with  
11 applicable industry standards constitutes an unfair act or practice prohibited by  
12 Section 5 of the FTC Act, 15 U.S.C. § 45.  
13

14           86. Upon information and belief, Defendant was at all times fully aware of  
15 its obligation to protect the PII of its clients’ employees, Defendant was also aware  
16 of the significant repercussions that would result from its failure to do so.  
17 Accordingly, Defendant’s conduct was particularly unreasonable given the nature  
18 and amount of PII it obtained and stored and the foreseeable consequences of the  
19 immense damages that would result to Plaintiff and the Class.  
20  
21

22           ***Defendant Fails to Comply with Industry Standards.***  
23

24           87. As noted above, experts studying cyber security routinely identify  
25 compliance companies in possession of PII as being particularly vulnerable to  
26 cyberattacks because of the value of the PII which they collect and maintain.  
27  
28

1        88. Several best practices have been identified that, at a minimum, should  
2 be implemented by compliance companies in possession of PII, like Defendant,  
3 including but not limited to: educating all employees; strong passwords; multi-layer  
4 security, including firewalls, anti-virus, and anti-malware software; encryption,  
5 making data unreadable without a key; multi-factor authentication; backup data and  
6 limiting which employees can access sensitive data. Defendant failed to follow these  
7 industry best practices, including a failure to implement multi-factor authentication.  
8  
9

10        89. Other best cybersecurity practices that are standard for compliance  
11 companies include installing appropriate malware detection software; monitoring  
12 and limiting the network ports; protecting web browsers and email management  
13 systems; setting up network systems such as firewalls, switches and routers;  
14 monitoring and protection of physical security systems; protection against any  
15 possible communication system; training staff regarding critical points. Defendant  
16 failed to follow these cybersecurity best practices, including failure to train staff.  
17  
18  
19

20        90. Defendant failed to meet the minimum standards of any of the  
21 following frameworks: the NIST Cybersecurity Framework Version 2.0 (including  
22 without limitation PR.AA-01, PR.AA-02, PR.AA-03, PR.AA-04, PR.AA-05,  
23 PR.AT-01, PR.DS-01, PR.DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05,  
24 PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04), and the  
25  
26  
27  
28

1 Center for Internet Security's Critical Security Controls (CIS CSC), which are all  
2 established standards in reasonable cybersecurity readiness.

3  
4 91. These foregoing frameworks are existing and applicable industry  
5 standards for compliance companies safeguarding their clients' employees' data, and  
6 upon information and belief, Defendant failed to comply with at least one—or all—  
7 of these accepted standards, thereby opening the door to the threat actor and causing  
8 the Data Breach.  
9

10 ***Common Injuries and Damages.***

11  
12 92. As a result of Defendant's ineffective and inadequate data security  
13 practices, the Data Breach, and the foreseeable consequences of PII ending up in the  
14 possession of criminals, the risk of identity theft to the Plaintiff and Class Members  
15 has materialized and is imminent, and Plaintiff and Class Members have all  
16 sustained actual injuries and damages, including: (i) invasion of privacy; (ii) theft of  
17 their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs  
18 associated with attempting to mitigate the actual consequences of the Data Breach;  
19 (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with  
20 attempting to mitigate the actual consequences of the Data Breach; (vii) statutory  
21 damages; (viii) nominal damages; and (ix) the continued and certainly increased risk  
22 to their PII, which: (a) remains unencrypted and available for unauthorized third  
23 parties to access and abuse; and (b) remains backed up in Defendant's possession  
24  
25  
26  
27  
28

1 and is subject to further unauthorized disclosures so long as Defendant fails to  
2 undertake appropriate and adequate measures to protect the PII.

3  
4 ***The Data Breach Increases Victims' Risk of Identity Theft.***

5 93. The unencrypted PII of Plaintiff and Class Members will end up for  
6 sale on the dark web as that is the *modus operandi* of hackers.

7  
8 94. Unencrypted PII may also fall into the hands of companies that will use  
9 the detailed PII for targeted marketing without the approval of Plaintiff and Class  
10 Members. Simply put, unauthorized individuals can easily access the PII of Plaintiff  
11 and Class Members.

12  
13 95. The link between a data breach and the risk of identity theft is simple  
14 and well established. Criminals acquire and steal PII to monetize the information.  
15 Criminals monetize the data by selling the stolen information on the black market to  
16 other criminals who then utilize the information to commit a variety of identity theft  
17 related crimes discussed below.

18  
19  
20 96. Plaintiff's and Class Members' PII is of great value to hackers and  
21 cyber criminals, and the data stolen in the Data Breach has been used and will  
22 continue to be used in a variety of sordid ways for criminals to exploit Plaintiff and  
23 Class Members and to profit off their misfortune.

24  
25 97. Due to the risk of one's Social Security number being exposed, state  
26 legislatures have passed laws in recognition of the risk: "[t]he social security number  
27  
28

1 can be used as a tool to perpetuate fraud against a person and to acquire sensitive  
2 personal, financial, medical, and familial information, the release of which could  
3 cause great financial or personal harm to an individual. While the social security  
4 number was intended to be used solely for the administration of the federal Social  
5 Security System, over time this unique numeric identifier has been used extensively  
6 for identity verification purposes[.]”<sup>27</sup>  
7  
8

9 98. Moreover, “SSNs have been central to the American identity  
10 infrastructure for years, being used as a key identifier[.] . . . U.S. banking processes  
11 have also had SSNs baked into their identification process for years. In fact, SSNs  
12 have been the gold standard for identifying and verifying the credit history of  
13 prospective customers.”<sup>28</sup>  
14  
15

16 99. “Despite the risk of fraud associated with the theft of Social Security  
17 numbers, just five of the nation’s largest 25 banks have stopped using the numbers  
18 to verify a customer’s identity after the initial account setup[.]”<sup>29</sup> Accordingly, since  
19 Social Security numbers are frequently used to verify an individual’s identity after  
20 logging onto an account or attempting a transaction, “[h]aving access to your Social  
21  
22  
23

---

24 <sup>27</sup> See N.C. Gen. Stat. § 132-1.10(1).  
25

26 <sup>28</sup> See <https://www.americanbanker.com/opinion/banks-need-to-stop-relying-on-social-security-numbers>

27 <sup>29</sup> See <https://archive.nytimes.com/bucks.blogs.nytimes.com/2013/03/20/just-5-banks-prohibit-use-of-social-security-numbers/>  
28

1 Security number may be enough to help a thief steal money from your bank  
2 account”<sup>30</sup>

3  
4 100. One such example of criminals piecing together bits and pieces of  
5 compromised PII for profit is the development of “Fullz” packages.<sup>31</sup>

6 101. With “Fullz” packages, cyber-criminals can cross-reference two  
7  
8 sources of PII to marry unregulated data available elsewhere to criminally stolen  
9 data with an astonishingly complete scope and degree of accuracy in order to  
10 assemble complete dossiers on individuals.

11  
12 102. The development of “Fullz” packages means here that the stolen PII  
13 from the Data Breach can easily be used to link and identify it to Plaintiff’s and Class  
14 Members’ phone numbers, email addresses, and other unregulated sources and  
15 identifiers. In other words, even if certain information such as emails, phone  
16

---

17  
18 <sup>30</sup> See <https://www.credit.com/blog/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/>

19 <sup>31</sup> “Fullz” is fraudster speak for data that includes the information of the victim, including, but not  
20 limited to, the name, address, credit card information, social security number, date of birth, and  
21 more. As a rule of thumb, the more information you have on a victim, the more money that can be  
22 made off of those credentials. Fullz are usually pricier than standard credit card credentials,  
23 commanding up to \$100 per record (or more) on the dark web. Fullz can be cashed out (turning  
24 credentials into money) in various ways, including performing bank transactions over the phone  
25 with the required authentication details in-hand. Even “dead Fullz,” which are Fullz credentials  
26 associated with credit cards that are no longer valid, can still be used for numerous purposes,  
27 including tax refund scams, ordering credit cards on behalf of the victim, or opening a “mule  
28 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/2014/09/medical-records-for-sale-in-underground-stolen-from-](https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-)  
[texas-life-insurance-\]\(https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-](https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/)  
[underground-stolen-from-texas-life-insurance-finn/](https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/)



1 numbers, or credit card numbers may not be included in the PII that was exfiltrated  
2 in the Data Breach, criminals may still easily create a Fullz package and sell it at a  
3 higher price to unscrupulous operators and criminals (such as illegal and scam  
4 telemarketers) over and over.

6 103. The existence and prevalence of “Fullz” packages means that the PII  
7 stolen from the data breach can easily be linked to the unregulated data (like  
8 insurance information) of Plaintiff and the other Class Members.

10 104. Thus, even if certain information (such as insurance information) was  
11 not stolen in the data breach, criminals can still easily create a comprehensive  
12 “Fullz” package.

14 105. Then, this comprehensive dossier can be sold—and then resold in  
15 perpetuity—to crooked operators and other criminals (like illegal and scam  
16 telemarketers).

18 ***Loss of Time to Mitigate the Risk of Identity Theft and Fraud.***

20 106. As a result of the recognized risk of identity theft, when a Data Breach  
21 occurs, and an individual is notified by a company that their PII was compromised,  
22 as in this Data Breach, the reasonable person is expected to take steps and spend  
23 time to address the dangerous situation, learn about the breach, and otherwise  
24 mitigate the risk of becoming a victim of identity theft or fraud. Failure to spend  
25

1 time taking steps to review accounts or credit reports could expose the individual to  
2 greater financial harm – yet the resource and asset of time has been lost.

3  
4 107. Thus, due to the actual and imminent risk of identity theft, Defendant,  
5 in its Notice Letter instructs Plaintiff and Class Members to take the following  
6 measures to protect themselves: “remain vigilant and review your account  
7 statements and free credit reports regularly to ensure there is no unauthorized or  
8 unexplained activity.”<sup>32</sup>

9  
10 108. In addition, Defendant’s Notice letter includes a full three pages  
11 devoted to “Steps You Can Take to Help Protect Personal Information” that  
12 recommend Plaintiff and Class Members to partake in activities such as enrolling in  
13 the credit monitoring services offered by Defendant, monitoring their accounts,  
14 placing fraud alerts on their accounts, and contacting consumer reporting bureaus.<sup>33</sup>

15  
16  
17 109. Defendant’s extensive suggestion of steps that Plaintiff and Class  
18 Members must take in order to protect themselves from identity theft and/or fraud  
19 demonstrates the significant time that Plaintiff and Class Members must undertake  
20 in response to the Data Breach. Plaintiff’s and Class Members’ time is highly  
21 valuable and irreplaceable, and accordingly, Plaintiff and Class Members suffered  
22 actual injury and damages in the form of lost time that they spent on mitigation  
23  
24  
25

---

26 <sup>32</sup> Notice Letter.

27 <sup>33</sup> *Id.*

1 activities in response to the Data Breach and at the direction of Defendant’s Notice  
2 Letter.

3  
4 110. Plaintiff and Class Members have spent, and will spend additional time  
5 in the future, on a variety of prudent actions, such as researching and verifying the  
6 legitimacy of the Data Breach. Accordingly, the Data Breach has caused Plaintiff  
7 and Class Members to suffer actual injury in the form of lost time—which cannot be  
8 recaptured—spent on mitigation activities.  
9

10 111. Plaintiff’s mitigation efforts are consistent with the U.S. Government  
11 Accountability Office that released a report in 2007 regarding data breaches (“GAO  
12 Report”) in which it noted that victims of identity theft will face “substantial costs  
13 and time to repair the damage to their good name and credit record.”<sup>34</sup>  
14  
15

16 112. Plaintiff’s mitigation efforts are also consistent with the steps that FTC  
17 recommends that data breach victims take several steps to protect their personal and  
18 financial information after a data breach, including: contacting one of the credit  
19 bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven  
20 years if someone steals their identity), reviewing their credit reports, contacting  
21  
22  
23  
24  
25

---

26 <sup>34</sup> See United States Government Accountability Office, GAO-07-737, Personal Information: Data  
27 Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full  
28 Extent Is Unknown (June 2007), <https://www.gao.gov/new.items/d07737.pdf>.

1 companies to remove fraudulent charges from their accounts, placing a credit freeze  
2 on their credit, and correcting their credit reports.<sup>35</sup>

3  
4 113. And for those Class Members who experience actual identity theft and  
5 fraud, the United States Government Accountability Office released a report in 2007  
6 regarding data breaches (“GAO Report”) in which it noted that victims of identity  
7 theft will face “substantial costs and time to repair the damage to their good name  
8 and credit record.”<sup>[4]</sup>

9  
10 ***Diminution of Value of PII.***

11  
12 114. PII is a valuable property right.<sup>36</sup> Its value is axiomatic, considering the  
13 value of Big Data in corporate America and the consequences of cyber thefts include  
14 heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond  
15 doubt that PII has considerable market value.

16  
17 115. Sensitive PII can sell for as much as \$363 per record according to the  
18 Infosec Institute.<sup>37</sup>

19  
20  
21  
22  
23 <sup>35</sup> See Federal Trade Commission, *Identity Theft.gov*, <https://www.identitytheft.gov/Steps> (last visited July 7, 2022).

24 <sup>36</sup> See “Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited;  
25 However, the Full Extent Is Unknown,” p. 2, U.S. Government Accountability Office, June 2007,  
<https://www.gao.gov/new.items/d07737.pdf> (last visited Sep. 13, 2022) (“GAO Report”).

26 <sup>37</sup> See, e.g., John T. Soma, et al, Corporate Privacy Trend: The “Value” of Personally Identifiable  
27 Information (“PII”) Equals the “Value” of Financial Assets, 15 Rich. J.L. & Tech. 11, at \*3-4  
28 (2009) (“PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching  
a level comparable to the value of traditional financial assets.”) (citations omitted).

1           116. An active and robust legitimate marketplace for PII also exists. In 2019,  
2 the data brokering industry was worth roughly \$200 billion.<sup>38</sup> In fact, the data  
3 marketplace is so sophisticated that consumers can actually sell their non-public  
4 information directly to a data broker who in turn aggregates the information and  
5 provides it to marketers or app developers.<sup>39,40</sup> Consumers who agree to provide their  
6 web browsing history to the Nielsen Corporation can receive up to \$50.00 a year.<sup>41</sup>  
7

9           117. As a result of the Data Breach, Plaintiff's and Class Members' PII ,  
10 which has an inherent market value in both legitimate and dark markets, has been  
11 damaged and diminished by its compromise and unauthorized release. However, this  
12 transfer of value occurred without any consideration paid to Plaintiff or Class  
13 Members for their property, resulting in an economic loss. Moreover, the PII is now  
14 readily available, and the rarity of the Data has been lost, thereby causing additional  
15 loss of value.  
16

18           118. At all relevant times, Defendant knew, or reasonably should have  
19 known, of the importance of safeguarding the PII of Plaintiff and Class Members,  
20 and of the foreseeable consequences that would occur if Defendant's data security  
21  
22  
23

24  
25 <sup>38</sup> See Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015),  
26 <https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/>  
(last visited Sep. 13, 2022).

27 <sup>39</sup> <https://www.latimes.com/business/story/2019-11-05/column-data-brokers>

28 <sup>40</sup> <https://datacoup.com/>

<sup>41</sup> <https://digi.me/what-is-digime/>

1 system was breached, including, specifically, the significant costs that would be  
2 imposed on Plaintiff and Class Members as a result of a breach.

3  
4 119. The fraudulent activity resulting from the Data Breach may not come  
5 to light for years.

6 120. Plaintiff and Class Members now face years of constant surveillance of  
7 their financial and personal records, monitoring, and loss of rights. The Class is  
8 incurring and will continue to incur such damages in addition to any fraudulent use  
9 of their PII .  
10

11  
12 121. Defendant was, or should have been, fully aware of the unique type and  
13 the significant volume of data on Defendant's network, amounting to more than  
14 twenty thousand individuals' detailed personal information and, thus, the significant  
15 number of individuals who would be harmed by the exposure of the unencrypted  
16 data.  
17

18 122. The injuries to Plaintiff and Class Members were directly and  
19 proximately caused by Defendant's failure to implement or maintain adequate data  
20 security measures for the PII of Plaintiff and Class Members.  
21

22 ***Future Costs of Credit and Identity Theft Monitoring is Reasonable and***  
23 ***Necessary.***

24 123. Given the type of targeted attack, the sophisticated criminal activity,  
25 and the type of PII involved in this case, there is a strong probability that entire  
26 batches of stolen information have been placed, or will be placed, on the black  
27  
28

1 market/dark web for sale and purchase by criminals intending to utilize the PII for  
2 identity theft crimes –e.g., opening bank accounts in the victims’ names to make  
3 purchases or to launder money; file false tax returns; take out loans or lines of credit;  
4 or file false unemployment claims.  
5

6 124. Such fraud may go undetected until debt collection calls commence  
7 months, or even years, later. An individual may not know that his or her PII was  
8 used to file for unemployment benefits until law enforcement notifies the  
9 individual’s employer of the suspected fraud. Fraudulent tax returns are typically  
10 discovered only when an individual’s authentic tax return is rejected.  
11  
12

13 125. Consequently, Plaintiff and Class Members are at an increased risk of  
14 fraud and identity theft for many years into the future.  
15

16 126. The retail cost of credit monitoring and identity theft monitoring can  
17 cost around \$200 a year per Class Member. This is reasonable and necessary cost to  
18 monitor to protect Class Members from the risk of identity theft that arose from  
19 Defendant’s Data Breach.  
20

21 ***Loss of Benefit of the Bargain.***  
22

23 127. Furthermore, Defendant’s poor data security deprived Plaintiff and  
24 Class Members of the benefit of their bargain. When agreeing to obtain employment  
25 at Defendant’s clients under certain terms, Plaintiff and other reasonable employees  
26 understood and expected that Defendant would properly safeguard and protect their  
27  
28

1 PII, when in fact, Defendant did not provide the expected data security. Accordingly,  
2 Plaintiff and Class Members received employment positions of a lesser value than  
3 what they reasonably expected to receive under the bargains they struck with  
4 Defendant's clients.  
5

6 ***Plaintiff Wilcopolski's Experience.***  
7

8 128. Plaintiff Wilcopolski is a former employee of Defendant's client.

9 129. As a condition of her employment at Defendant's client, she was  
10 required to supply Defendant with her PII, including but not limited to her name,  
11 address, date of birth, and Social Security number.  
12

13 130. Plaintiff Wilcopolski is very careful about sharing her sensitive PII.  
14 Plaintiff stores any documents containing her PII in a safe and secure location.  
15 She has never knowingly transmitted unencrypted sensitive PII over the internet  
16 or any other unsecured source.  
17

18 131. At the time of the Data Breach—on or about February 5, 2024—  
19 Defendant retained Plaintiff's PII in its system.  
20

21 132. Plaintiff Wilcopolski received the Notice Letter, by U.S. mail,  
22 directly from Defendant, dated May 31, 2024. According to the Notice Letter,  
23 Plaintiff's PII was improperly accessed and obtained by unauthorized third  
24 parties, including her full name, address, date of birth, hire date, and Social  
25 Security number.  
26  
27  
28



1           133. As a result of the Data Breach, and at the direction of Defendant's  
2 Notice Letter, which instructs Plaintiff to "remain vigilant and review your  
3 account statements and free credit reports regularly to ensure there is no  
4 unauthorized or unexplained activity[,]"<sup>42</sup> Plaintiff made reasonable efforts to  
5 mitigate the impact of the Data Breach, including but not limited to: researching  
6 and verifying the legitimacy of the Data Breach. Plaintiff have spent significant  
7 on mitigation activities in response to the Data Breach—valuable time Plaintiff  
8 otherwise would have spent on other activities, including but not limited to work  
9 and/or recreation. This time has been lost forever and cannot be recaptured.  
10

11  
12  
13           134. Subsequent to the Data Breach, Plaintiff Wilcopolski has suffered  
14 numerous, substantial injuries including, but not limited to: (i) invasion of  
15 privacy; (ii) theft of her PII; (iii) lost or diminished value of PII; (iv) lost time  
16 and opportunity costs associated with attempting to mitigate the actual  
17 consequences of the Data Breach; (v) lost opportunity costs associated with  
18 attempting to mitigate the actual consequences of the Data Breach; (vi) statutory  
19 damages; (vii) nominal damages; and (viii) the continued and certainly increased  
20 risk to her PII, which: (a) remains unencrypted and available for unauthorized  
21 third parties to access and abuse; and (b) remains backed up in Defendant's  
22  
23  
24  
25  
26

---

27 <sup>42</sup> Notice Letter.  
28

1 possession and is subject to further unauthorized disclosures so long as Defendant  
2 fails to undertake appropriate and adequate measures to protect the PII.

3  
4 135. Plaintiff also suffered actual injury in the form of experiencing an  
5 increase in spam calls, texts, and/or emails, which, upon information and belief,  
6 was caused by the Data Breach. This misuse of her PII was caused, upon  
7 information and belief, by the fact that cybercriminals are able to easily use the  
8 information compromised in the Data Breach to find more information about an  
9 individual, such as their phone number or email address, from publicly available  
10 sources, including websites that aggregate and associate personal information  
11 with the owner of such information. Criminals often target data breach victims  
12 with spam emails, calls, and texts to gain access to their devices with phishing  
13 attacks or elicit further personal information for use in committing identity theft  
14 or fraud.  
15

16  
17  
18 136. The Data Breach has caused Plaintiff to suffer fear, anxiety, and  
19 stress, which has been compounded by the fact that Defendant has still not fully  
20 informed her of key details about the Data Breach's occurrence.  
21

22 137. As a result of the Data Breach, Plaintiff anticipates spending  
23 considerable time and money on an ongoing basis to try to mitigate and address  
24 harms caused by the Data Breach.  
25  
26  
27  
28

1           138. As a result of the Data Breach, Plaintiff is at a present risk and will  
2 continue to be at increased risk of identity theft and fraud for years to come.

3  
4           139. Plaintiff Wilcopolski has a continuing interest in ensuring that her  
5 PII, which, upon information and belief, remains backed up in Defendant's  
6 possession, is protected and safeguarded from future breaches.

7  
8                           **CLASS ACTION ALLEGATIONS**

9           140. Plaintiff brings this nationwide class action on behalf of herself and on  
10 behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and  
11 23(c)(4) of the Federal Rules of Civil Procedure.

12  
13           141.       The Class that Plaintiff seeks to represent is defined as follows:

14           All individuals residing in the United States whose PII was accessed and/or  
15 acquired by an unauthorized party as a result of the data breach reported by  
16 Defendant in May 2024 (the "Class").

17           142. Excluded from the Class are the following individuals and/or entities:  
18 Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors,  
19 and any entity in which Defendant have a controlling interest; all individuals who  
20 make a timely election to be excluded from this proceeding using the correct protocol  
21 for opting out; and all judges assigned to hear any aspect of this litigation, as well as  
22 their immediate family members.  
23  
24  
25  
26  
27  
28

1           143. Plaintiff reserves the right to amend the definitions of the Class or add  
2 a Class or Subclass if further information and discovery indicate that the definitions  
3 of the Class should be narrowed, expanded, or otherwise modified.  
4

5           144. Numerosity. The members of the Class are so numerous that joinder of  
6 all members is impracticable, if not completely impossible. At least 27,000  
7 individuals were notified by Defendant of the Data Breach, according to the breach  
8 report submitted to Maine Attorney General's Office.<sup>43</sup> The Class is apparently  
9 identifiable within Defendant's records, and Defendant has already identified these  
10 individuals (as evidenced by sending them breach notification letters).  
11  
12

13           145. Common questions of law and fact exist as to all members of the Class  
14 and predominate over any questions affecting solely individual members of the  
15 Class. Among the questions of law and fact common to the Class that predominate  
16 over questions which may affect individual Class members, including the following:  
17

- 18           a. Whether and to what extent Defendant had a duty to protect the PII of  
19 Plaintiff and Class Members;  
20  
21           b. Whether Defendant had respective duties not to disclose the PII of  
22 Plaintiff and Class Members to unauthorized third parties;  
23  
24  
25  
26

---

27 <sup>43</sup> [https://apps.web.maine.gov/online/aevviewer/ME/40/c0ea4ec7-a813-433b-b966-](https://apps.web.maine.gov/online/aevviewer/ME/40/c0ea4ec7-a813-433b-b966-e1201d2b92ca.shtml)  
28 [e1201d2b92ca.shtml](https://apps.web.maine.gov/online/aevviewer/ME/40/c0ea4ec7-a813-433b-b966-e1201d2b92ca.shtml)

- c. Whether Defendant had respective duties not to use the PII of Plaintiff and Class Members for non-business purposes;
- d. Whether Defendant failed to adequately safeguard the PII of Plaintiff and Class Members;
- e. Whether and when Defendant actually learned of the Data Breach;
- f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;
- g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;
- h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;
- j. Whether Plaintiff and Class Members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Defendant's wrongful conduct; and,
- k. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

1       146. Typicality. Plaintiff's claims are typical of those of the other members  
2 of the Class because Plaintiff, like every other Class Member, was exposed to  
3 virtually identical conduct and now suffers from the same violations of the law as  
4 each other member of the Class.  
5

6       147. Policies Generally Applicable to the Class. This class action is also  
7 appropriate for certification because Defendant acted or refused to act on grounds  
8 generally applicable to the Class, thereby requiring the Court's imposition of  
9 uniform relief to ensure compatible standards of conduct toward the Class Members  
10 and making final injunctive relief appropriate with respect to the Class as a whole.  
11 Defendant's policies challenged herein apply to and affect Class Members uniformly  
12 and Plaintiff's challenge of these policies hinges on Defendant's conduct with  
13 respect to the Class as a whole, not on facts or law applicable only to Plaintiff.  
14  
15  
16

17       148. Adequacy. Plaintiff will fairly and adequately represent and protect the  
18 interests of the Class Members in that she has no disabling conflicts of interest that  
19 would be antagonistic to those of the other Class Members. Plaintiff seeks no relief  
20 that is antagonistic or adverse to the Class Members and the infringement of the  
21 rights and the damages she has suffered are typical of other Class Members. Plaintiff  
22 has retained counsel experienced in complex class action and data breach litigation,  
23 and Plaintiff intends to prosecute this action vigorously.  
24  
25  
26  
27  
28

1           149. Superiority and Manageability. The class litigation is an appropriate  
2 method for fair and efficient adjudication of the claims involved. Class action  
3 treatment is superior to all other available methods for the fair and efficient  
4 adjudication of the controversy alleged herein; it will permit a large number of Class  
5 Members to prosecute their common claims in a single forum simultaneously,  
6 efficiently, and without the unnecessary duplication of evidence, effort, and expense  
7 that hundreds of individual actions would require. Class action treatment will permit  
8 the adjudication of relatively modest claims by certain Class Members, who could  
9 not individually afford to litigate a complex claim against large corporations, like  
10 Defendant. Further, even for those Class Members who could afford to litigate such  
11 a claim, it would still be economically impractical and impose a burden on the courts.  
12

13           150. The nature of this action and the nature of laws available to Plaintiff  
14 and Class Members make the use of the class action device a particularly efficient  
15 and appropriate procedure to afford relief to Plaintiff and Class Members for the  
16 wrongs alleged because Defendant would necessarily gain an unconscionable  
17 advantage since they would be able to exploit and overwhelm the limited resources  
18 of each individual Class Member with superior financial and legal resources; the  
19 costs of individual suits could unreasonably consume the amounts that would be  
20 recovered; proof of a common course of conduct to which Plaintiff was exposed is  
21 representative of that experienced by the Class and will establish the right of each  
22  
23  
24  
25  
26  
27  
28

1 Class Member to recover on the cause of action alleged; and individual actions  
2 would create a risk of inconsistent results and would be unnecessary and duplicative  
3 of this litigation.  
4

5 151. The litigation of the claims brought herein is manageable. Defendant's  
6 uniform conduct, the consistent provisions of the relevant laws, and the ascertainable  
7 identities of Class Members demonstrates that there would be no significant  
8 manageability problems with prosecuting this lawsuit as a class action.  
9

10 152. Adequate notice can be given to Class Members directly using  
11 information maintained in Defendant's records.  
12

13 153. Unless a Class-wide injunction is issued, Defendant may continue in its  
14 failure to properly secure the PII of Class Members, Defendant may continue to  
15 refuse to provide proper notification to Class Members regarding the Data Breach,  
16 and Defendant may continue to act unlawfully as set forth in this Complaint.  
17

18 154. Further, Defendant has acted on grounds that apply generally to the  
19 Class as a whole, so that class certification, injunctive relief, and corresponding  
20 declaratory relief are appropriate on a class- wide basis.  
21

22 155. Likewise, particular issues under Rule 23(c)(2) are appropriate for  
23 certification because such claims present only particular, common issues, the  
24 resolution of which would advance the disposition of this matter and the parties'  
25 interests therein. Such particular issues include, but are not limited to:  
26  
27  
28



- a. Whether Defendant failed to timely notify the Plaintiff and the class of the Data Breach;
- b. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;
- c. Whether Defendant's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;
- d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;
- e. Whether Defendant failed to take commercially reasonable steps to safeguard its clients' employees' PII; and,
- f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

## **CAUSES OF ACTION**

### **COUNT I NEGLIGENCE**

#### **(On Behalf of Plaintiff and All Class Members)**

156. Plaintiff re-alleges and incorporates by reference all of the preceding allegations, as if fully set forth herein.

1           157. Defendant requires its clients' employees, including Plaintiff and Class  
2 Members, to submit non-public PII in the ordinary course of providing its services.

3  
4           158. Defendant gathered and stored the PII of Plaintiff and Class Members  
5 as part of its business of soliciting its clients' employees, which solicitations and  
6 services affect commerce.

7  
8           159. Plaintiff and Class Members entrusted Defendant with their PII with  
9 the understanding that Defendant would safeguard their information.

10           160. Defendant had full knowledge of the sensitivity of the PII and the types  
11 of harm that Plaintiff and Class Members could and would suffer if the PII were  
12 wrongfully disclosed.

13  
14           161. By assuming the responsibility to collect and store this data, and in fact  
15 doing so, and sharing it and using it for commercial gain, Defendant had a duty of  
16 care to use reasonable means to secure and to prevent disclosure of the information,  
17 and to safeguard the information from theft.

18  
19  
20           162. Defendant had a duty to employ reasonable security measures under  
21 Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits  
22 "unfair . . . practices in or affecting commerce," including, as interpreted and  
23 enforced by the FTC, the unfair practice of failing to use reasonable measures to  
24 protect confidential data.  
25  
26  
27  
28

1           163. Defendant owed a duty of care to Plaintiff and Class Members to  
2 provide data security consistent with industry standards and other requirements  
3 discussed herein, and to ensure that its systems and networks, and the personnel  
4 responsible for them, adequately protected the PII.  
5

6           164. Defendant's duty of care to use reasonable security measures arose as a  
7 result of the special relationship that existed between Defendant and Plaintiff and  
8 Class Members. That special relationship arose because Plaintiff and the Class  
9 entrusted Defendant with their confidential PII, a necessary part of obtaining  
10 employment at Defendant's clients.  
11  
12

13           165. Defendant's duty to use reasonable care in protecting confidential data  
14 arose not only as a result of the statutes and regulations described above, but also  
15 because Defendant is bound by industry standards to protect confidential PII.  
16

17           166. Defendant was subject to an "independent duty," untethered to any  
18 contract between Defendant and Plaintiff or the Class.  
19

20           167. Defendant also had a duty to exercise appropriate clearinghouse  
21 practices to remove former employees' PII it was no longer required to retain  
22 pursuant to regulations.  
23

24           168. Moreover, Defendant had a duty to promptly and adequately notify  
25 Plaintiff and the Class of the Data Breach.  
26  
27  
28

1           169. Defendant had and continues to have a duty to adequately disclose that  
2 the PII of Plaintiff and the Class within Defendant's possession might have been  
3 compromised, how it was compromised, and precisely the types of data that were  
4 compromised and when. Such notice was necessary to allow Plaintiff and the Class  
5 to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use  
6 of their PII by third parties.  
7

8  
9           170. Defendant breached its duties, pursuant to the FTC Act and other  
10 applicable standards, and thus was negligent, by failing to use reasonable measures  
11 to protect Class Members' PII. The specific negligent acts and omissions committed  
12 by Defendant include, but are not limited to, the following:  
13

- 14           a. Failing to adopt, implement, and maintain adequate security measures  
15           to safeguard Class Members' PII;
- 16           b. Failing to adequately monitor the security of their networks and  
17           systems;
- 18           c. Allowing unauthorized access to Class Members' PII;
- 19           d. Failing to detect in a timely manner that Class Members' PII had been  
20           compromised;
- 21           e. Failing to remove former employees' PII it was no longer required to  
22           retain pursuant to regulations, and;
- 23           f. Failing to timely and adequately notify Class Members about the Data  
24  
25  
26  
27  
28

1 Breach's occurrence and scope, so that they could take appropriate  
2 steps to mitigate the potential for identity theft and other damages.  
3

4 171. Defendant violated Section 5 of the FTC Act by failing to use  
5 reasonable measures to protect PII and not complying with applicable industry  
6 standards, as described in detail herein. Defendant's conduct was particularly  
7 unreasonable given the nature and amount of PII it obtained and stored and the  
8 foreseeable consequences of the immense damages that would result to Plaintiff and  
9 the Class.  
10

11 172. Defendant's violation of Section 5 of the FTC Act constitutes  
12 negligence.  
13

14 173. Plaintiff and Class Members were within the class of persons the  
15 Federal Trade Commission Act was intended to protect and the type of harm that  
16 resulted from the Data Breach was the type of harm the statute was intended to guard  
17 against.  
18

19 174. The FTC has pursued enforcement actions against businesses, which,  
20 as a result of their failure to employ reasonable data security measures and avoid  
21 unfair and deceptive practices, caused the same harm as that suffered by Plaintiff  
22 and the Class.  
23  
24  
25  
26  
27  
28

1 175. A breach of security, unauthorized access, and resulting injury to  
2 Plaintiff and the Class was reasonably foreseeable, particularly in light of  
3 Defendant's inadequate security practices.  
4

5 176. It was foreseeable that Defendant's failure to use reasonable measures  
6 to protect Class Members' PII would result in injury to Class Members. Further, the  
7 breach of security was reasonably foreseeable given the known high frequency of  
8 cyberattacks and data breaches targeting compliance companies in possession of PII.  
9

10 177. Defendant has full knowledge of the sensitivity of the PII and the types  
11 of harm that Plaintiff and the Class could and would suffer if the PII were wrongfully  
12 disclosed.  
13

14 178. Plaintiff and the Class were the foreseeable and probable victims of any  
15 inadequate security practices and procedures. Defendant knew or should have  
16 known of the inherent risks in collecting and storing the PII of Plaintiff and the Class,  
17 the critical importance of providing adequate security of that PII, and the necessity  
18 for encrypting PII stored on Defendant's systems.  
19

20 179. It was therefore foreseeable that the failure to adequately safeguard  
21 Class Members' PII would result in one or more types of injuries to Class Members.  
22

23 180. Plaintiff and the Class had no ability to protect their PII that was in, and  
24 possibly remains in, Defendant's possession.  
25  
26  
27  
28

1 181. Defendant was in a position to protect against the harm suffered by  
2 Plaintiff and the Class as a result of the Data Breach.

3  
4 182. Defendant's duty extended to protecting Plaintiff and the Class from  
5 the risk of foreseeable criminal conduct of third parties, which has been recognized  
6 in situations where the actor's own conduct or misconduct exposes another to the  
7 risk or defeats protections put in place to guard against the risk, or where the parties  
8 are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous  
9 courts and legislatures have also recognized the existence of a specific duty to  
10 reasonably safeguard personal information.  
11  
12

13 183. Defendant has admitted that the PII of Plaintiff and the Class was  
14 wrongfully lost and disclosed to unauthorized third persons as a result of the Data  
15 Breach.  
16

17 184. But for Defendant's wrongful and negligent breach of duties owed to  
18 Plaintiff and the Class, the PII of Plaintiff and the Class would not have been  
19 compromised.  
20

21 185. There is a close causal connection between Defendant's failure to  
22 implement security measures to protect the PII of Plaintiff and the Class and the  
23 harm, or risk of imminent harm, suffered by Plaintiff and the Class. The PII of  
24 Plaintiff and the Class was lost and accessed as the proximate result of Defendant's  
25  
26  
27  
28

1 failure to exercise reasonable care in safeguarding such PII by adopting,  
2 implementing, and maintaining appropriate security measures.

3  
4 186. As a direct and proximate result of Defendant's negligence, Plaintiff  
5 and the Class have suffered and will suffer injury, including but not limited to: (i)  
6 invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv)  
7 lost time and opportunity costs associated with attempting to mitigate the actual  
8 consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost  
9 opportunity costs associated with attempting to mitigate the actual consequences of  
10 the Data Breach; (vii) actual misuse of the compromised data consisting of an  
11 increase in spam calls, texts, and/or emails; (viii) nominal damages; and (ix) the  
12 continued and certainly increased risk to their PII, which: (a) remains unencrypted  
13 and available for unauthorized third parties to access and abuse; and (b) remains  
14 backed up in Defendant's possession and is subject to further unauthorized  
15 disclosures so long as Defendant fails to undertake appropriate and adequate  
16 measures to protect the PII.  
17

18  
19  
20  
21 187. As a direct and proximate result of Defendant's negligence, Plaintiff  
22 and the Class have suffered and will continue to suffer other forms of injury and/or  
23 harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and  
24 other economic and non-economic losses.  
25  
26  
27  
28



1 188. Additionally, as a direct and proximate result of Defendant's  
2 negligence, Plaintiff and the Class have suffered and will suffer the continued risks  
3 of exposure of their PII, which remain in Defendant's possession and is subject to  
4 further unauthorized disclosures so long as Defendant fails to undertake appropriate  
5 and adequate measures to protect the PII in its continued possession.  
6

7  
8 189. Plaintiff and Class Members are entitled to compensatory and  
9 consequential damages suffered as a result of the Data Breach.

10 190. Defendant's negligent conduct is ongoing, in that it still holds the PII  
11 of Plaintiff and Class Members in an unsafe and insecure manner.  
12

13 191. Plaintiff and Class Members are also entitled to injunctive relief  
14 requiring Defendant to (i) strengthen its data security systems and monitoring  
15 procedures; (ii) submit to future annual audits of those systems and monitoring  
16 procedures; and (iii) continue to provide adequate credit monitoring to all Class  
17 Members.  
18

19  
20 **COUNT II**  
21 **BREACH OF THIRD-PARTY BENEFICIARY CONTRACT**  
22 **(On Behalf of Plaintiff and All Class Members)**

23 192. Plaintiff re-alleges and incorporates by reference all of the preceding  
24 allegations, as if fully set forth herein.

25 193. Defendant entered into written contracts with its clients to provide  
26 compliance services.  
27  
28

1           194. In exchange, Defendant agreed, in part, to implement adequate security  
2 measures to safeguard the PII of Plaintiff and the Class and to timely and adequately  
3 notify them of the Data Breach.  
4

5           195. These contracts were made expressly for the benefit of Plaintiff and the  
6 Class, as Plaintiff and Class Members were the intended third-party beneficiaries of  
7 the contracts entered into between Defendant and its clients. Defendant knew that,  
8 if it were to breach these contracts with its clients, the its clients' employees—  
9 Plaintiff and Class Members—would be harmed.  
10

11           196. Defendant breached the contracts it entered into with its clients by,  
12 among other things, failing to (i) use reasonable data security measures, (ii)  
13 implement adequate protocols and employee training sufficient to protect Plaintiff's  
14 PII from unauthorized disclosure to third parties, and (iii) promptly and adequately  
15 notify Plaintiff and Class Members of the Data Breach.  
16

17           197. Plaintiff and the Class were harmed by Defendant's breach of its  
18 contracts with its clients, as such breach is alleged herein, and are entitled to the  
19 losses and damages they have sustained as a direct and proximate result thereof.  
20

21           198. Plaintiff and Class Members are also entitled to their costs and  
22 attorney's fees incurred in this action.  
23  
24  
25  
26  
27  
28

**COUNT III**  
**UNJUST ENRICHMENT**  
**(On Behalf of Plaintiff and All Class Members)**

199. Plaintiff re-alleges and incorporates by reference all of the preceding allegations, as if fully set forth herein.

200. This Count is pleaded in the alternative to the breach of third-party beneficiary contract claim above.

201. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they provided Defendant with their PII. In exchange, Plaintiff and Class Members should have had their PII protected with adequate data security.

202. Defendant knew that Plaintiff and Class Members conferred a benefit upon it and has accepted and retained that benefit by accepting and retaining the PII entrusted to it. Defendant profited from Plaintiff's retained data and used Plaintiff's and Class Members' PII for business purposes.

203. Defendant failed to secure Plaintiff's and Class Members' PII and, therefore, did not fully compensate Plaintiff or Class Members for the value that their PII provided.

204. Defendant acquired the PII through inequitable record retention as it failed to investigate and/or disclose the inadequate data security practices previously alleged.

1        205. If Plaintiff and Class Members had known that Defendant would not  
2 use adequate data security practices, procedures, and protocols to adequately  
3 monitor, supervise, and secure their PII, they would have entrusted their PII at  
4 Defendant or obtained employment at Defendant's clients.  
5

6        206. Plaintiff and Class Members have no adequate remedy at law.  
7

8        207. Defendant enriched itself by saving the costs it reasonably should have  
9 expended on data security measures to secure Plaintiff's and Class Members'  
10 Personal Information. Instead of providing a reasonable level of security that would  
11 have prevented the hacking incident, Defendant instead calculated to increase its  
12 own profit at the expense of Plaintiff and Class Members by utilizing cheaper,  
13 ineffective security measures and diverting those funds to its own profit. Plaintiff  
14 and Class Members, on the other hand, suffered as a direct and proximate result of  
15 Defendant's decision to prioritize its own profits over the requisite security and the  
16 safety of their PII.  
17  
18  
19

20        208. Under the circumstances, it would be unjust for Defendant to be  
21 permitted to retain any of the benefits that Plaintiff and Class Members conferred  
22 upon it.  
23

24        209. As a direct and proximate result of Defendant's conduct, Plaintiff and  
25 Class Members have suffered and will suffer injury, including but not limited to: (i)  
26 invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv)  
27  
28

1 lost time and opportunity costs associated with attempting to mitigate the actual  
2 consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost  
3 opportunity costs associated with attempting to mitigate the actual consequences of  
4 the Data Breach; (vii) actual misuse of the compromised data consisting of an  
5 increase in spam calls, texts, and/or emails; (viii) nominal damages; and (ix) the  
6 continued and certainly increased risk to their PII, which: (a) remains unencrypted  
7 and available for unauthorized third parties to access and abuse; and (b) remains  
8 backed up in Defendant's possession and is subject to further unauthorized  
9 disclosures so long as Defendant fails to undertake appropriate and adequate  
10 measures to protect the PII.  
11  
12  
13

14         210. Plaintiff and Class Members are entitled to full refunds, restitution,  
15 and/or damages from Defendant and/or an order proportionally disgorging all  
16 profits, benefits, and other compensation obtained by Defendant from its wrongful  
17 conduct. This can be accomplished by establishing a constructive trust from which  
18 the Plaintiff and Class Members may seek restitution or compensation.  
19  
20

21         211. Plaintiff and Class Members may not have an adequate remedy at law  
22 against Defendant, and accordingly, they plead this claim for unjust enrichment in  
23 addition to, or in the alternative to, other claims pleaded herein.  
24  
25  
26  
27  
28

**COUNT IV**  
**VIOLATIONS OF CALIFORNIA’S UNFAIR COMPETITION LAW**  
**(“UCL”), UNLAWFUL BUSINESS PRACTICE**  
**Cal Bus. & Prof. Code § 17200, *et seq.***  
**(On Behalf of Plaintiff and All Class Members)**

212. Plaintiff re-alleges and incorporates by reference all of the preceding allegations, as if fully set forth herein.

213. Defendant is a “person” defined by Cal. Bus. & Prof. Code § 17201.

214. Defendant violated Cal. Bus. & Prof. Code § 17200 *et seq.* (“UCL”) by engaging in unlawful, unfair, and deceptive business acts and practices.

215. Defendant’s “unfair” acts and practices include:

- a. by utilizing cheaper, ineffective security measures and diverting those funds to its own profit, instead of providing a reasonable level of security that would have prevented the hacking incident;
- b. failing to follow industry standard and the applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data;
- c. failing to timely and adequately notify Class Members about the Data Breach’s occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages;

1 d. Omitting, suppressing, and concealing the material fact that it did not  
2 reasonably or adequately secure Plaintiff's and Class Members' personal  
3 information; and  
4

5 e. Omitting, suppressing, and concealing the material fact that it did not  
6 comply with common law and statutory duties pertaining to the security  
7 and privacy of Plaintiff's and Class Members' personal information,  
8 including duties imposed by the FTC Act, 15 U.S.C. § 45.  
9

10 216. Defendant has engaged in "unlawful" business practices by violating  
11 multiple laws, including the FTC Act, 15 U.S.C. § 45, and California common law.  
12

13 217. Defendant's unlawful, unfair, and deceptive acts and practices include:

14 a. Failing to implement and maintain reasonable security and privacy  
15 measures to protect Plaintiff's and Class Members' personal information,  
16 which was a direct and proximate cause of the Data Breach;  
17

18 b. Failing to identify foreseeable security and privacy risks, remediate  
19 identified security and privacy risks, which was a direct and proximate  
20 cause of the Data Breach;  
21

22 c. Failing to comply with common law and statutory duties pertaining to the  
23 security and privacy of Plaintiff's and Class Members' personal  
24 information, including duties imposed by the FTC Act, 15 U.S.C. § 45,  
25 which was a direct and proximate cause of the Data Breach;  
26  
27  
28

- 1 d. Misrepresenting that it would protect the privacy and confidentiality of  
2 Plaintiff's and Class Members' personal information, including by  
3 implementing and maintaining reasonable security measures; and  
4  
5 e. Misrepresenting that it would comply with common law and statutory  
6 duties pertaining to the security and privacy of Plaintiff's and Class  
7 Members' personal information, including duties imposed by the FTC Act,  
8 15 U.S.C. § 45.  
9

10 218. Defendant's representations and omissions were material because they  
11 were likely to deceive reasonable consumers about the adequacy of Defendant's data  
12 security and ability to protect the confidentiality of consumers' personal information.  
13

14 219. As a direct and proximate result of Defendant's unfair, unlawful, and  
15 fraudulent acts and practices, Plaintiff and Class Members' were injured and lost  
16 money or property, which would not have occurred but for the unfair and deceptive  
17 acts, practices, and omissions alleged herein, time and expenses related to  
18 monitoring their financial accounts for fraudulent activity, an increased, imminent  
19 risk of fraud and identity theft, and loss of value of their personal information.  
20  
21

22 220. Defendant's violations were, and are, willful, deceptive, unfair, and  
23 unconscionable.  
24

25 221. Plaintiff and Class Members have lost money and property as a result  
26 of Defendant's conduct in violation of the UCL, as stated herein and above.  
27  
28





1 to issue prompt, complete, any accurate disclosures to Plaintiff and  
2 Class Members;

3  
4 C. For injunctive relief requested by Plaintiff, including but not limited to,  
5 injunctive and other equitable relief as is necessary to protect the  
6 interests of Plaintiff and Class Members, including but not limited to  
7 an order:  
8

9 i. prohibiting Defendant from engaging in the wrongful and  
10 unlawful acts described herein;

11  
12 ii. requiring Defendant to protect, including through encryption, all  
13 data collected through the course of its business in accordance  
14 with all applicable regulations, industry standards, and federal,  
15 state, or local laws.  
16

17 iii. requiring Defendant to delete, destroy, and purge the personal  
18 identifying information of Plaintiff and Class Members unless  
19 Defendant can provide to the Court reasonable justification for  
20 the retention and use of such information when weighed against  
21 the privacy interests of Plaintiff and Class Members;  
22

23  
24 iv. requiring Defendant to implement and maintain a comprehensive  
25 Information Security Program designed to protect the  
26  
27  
28

1 confidentiality and integrity of the PII of Plaintiff and Class  
2 Members;

3  
4 v. prohibiting Defendant from maintaining the PII of Plaintiff and  
5 Class Members on a cloud-based database;

6 Vi. requiring Defendant to engage independent third-party security  
7 auditors/penetration testers as well as internal security personnel  
8 to conduct testing, including simulated attacks, penetration tests,  
9 and audits on Defendant's systems on a periodic basis, and  
10 ordering Defendant to promptly correct any problems or issues  
11 detected by such third-party security auditors;

12  
13  
14 vii. requiring Defendant to engage independent third-party security  
15 auditors and internal personnel to run automated security  
16 monitoring;

17  
18 viii. requiring Defendant to audit, test, and train its security personnel  
19 regarding any new or modified procedures;

20  
21 ix. requiring Defendant to segment data by, among other things,  
22 creating firewalls and access controls so that if one area of  
23 Defendant's network is compromised, hackers cannot gain  
24 access to other portions of Defendant's systems;  
25  
26  
27  
28

- x. requiring Defendant to conduct regular database scanning and securing checks;
- xi. requiring Defendant 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 personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;
- xii. requiring Defendant to conduct internal training and education routinely and continually, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;
- xiii. requiring Defendant to implement a system of tests to assess its employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

1           xiv. requiring Defendant to implement, maintain, regularly review,  
2                   and revise as necessary a threat management program designed  
3                   to appropriately monitor Defendant's information networks for  
4                   threats, both internal and external, and assess whether  
5                   monitoring tools are appropriately configured, tested, and  
6                   updated;  
7

8  
9           xv. requiring Defendant to meaningfully educate all Class Members  
10                   about the threats that they face as a result of the loss of their  
11                   confidential PII to third parties, as well as the steps affected  
12                   individuals must take to protect themselves;  
13

14           xvi. requiring Defendant to implement logging and monitoring  
15                   programs sufficient to track traffic to and from Defendant's  
16                   servers; and for a period of 10 years, appointing a qualified and  
17                   independent third-party assessor to conduct a SOC 2 Type 2  
18                   attestation on an annual basis to evaluate Defendant's  
19                   compliance with the terms of the Court's final judgment, to  
20                   provide such report to the Court and to counsel for the class, and  
21                   to report any deficiencies with compliance of the Court's final  
22                   judgment;  
23  
24  
25  
26  
27  
28

1 D. For an award of damages, including actual, statutory, nominal, and  
2 consequential damages, as allowed by law in an amount to be determined;

3  
4 E. For an award of attorneys' fees and costs as allowed by law;

5 F. For prejudgment interest on all amounts awarded; and

6 G. Such other and further relief as this Court may deem just and proper.  
7

8 **JURY TRIAL DEMANDED**

9 Plaintiff, individually and on behalf of the Class, hereby demands a trial by  
10 jury on all claims so triable.  
11

12 Dated: June 12, 2024

By: /s/ John J. Nelson  
John J. Nelson (SBN 317598)  
**MILBERG COLEMAN BRYSON**  
**PHILLIPS GROSSMAN, PLLC**  
280 S. Beverly Drive  
Beverly Hills, CA 90212  
Telephone: (858) 209-6941  
Email: jnelson@milberg.com

17  
18 *Attorney for Plaintiff and*  
19 *the Putative Class*  
20  
21  
22  
23  
24  
25  
26  
27  
28

# ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [February 2024 Form I-9 Compliance Data Breach Sparks Class Action Lawsuit](#)

---