

**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF COLORADO**

Civil Action No. 23-cv-00408-GPG-MEH

DIANE S. JONES, and  
JOAN OGG, *on behalf of themselves and all others similarly situated*,

Plaintiffs,

v.

P2ES HOLDINGS, LLC d/b/a P2 Energy Solutions,

Defendant.

---

**CONSOLIDATED AMENDED CLASS ACTION COMPLAINT AND JURY TRIAL  
DEMAND**

---

Plaintiffs Diane S. Jones and Joan Ogg (“Plaintiffs”), on behalf of themselves and all others similarly situated, bring this Class Action Complaint against P2ES Holdings, LLC dba P2 Energy Solutions (“Defendant” or “P2”), and allege, upon personal knowledge as to their own actions and their counsels’ investigations, and upon information and belief as to all other matters, as follows:

**I. INTRODUCTION**

1. This class action arises out of the recent targeted cyberattack and data breach on Defendant’s computer networks that resulted in unauthorized access and exfiltration of highly sensitive personally identifiable information (“PII”)<sup>1</sup>.

---

<sup>1</sup> Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on its face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong

2. Defendant is the world's largest independent provider of software and data solutions exclusively serving the upstream oil and gas industry. Defendant's headquarters is located in Denver, Colorado.

3. Defendant acquires, processes, analyzes, and otherwise utilizes Plaintiffs' and Class Members' PII, including, but not limited to, names and Social Security numbers in the course of providing software and data solutions to its clients.

4. In its required notice letter, sent to state and federal agencies and some Class Members, Defendant states that it identified suspicious activity on its computer network (the "Data Breach") on November 11, 2021, and through its subsequent investigation Defendant learned that an unauthorized party accessed and acquired certain files from its network.<sup>2</sup>

5. Defendant did not notify Plaintiffs and Class Members until on or around January 13, 2023 ("Notice Letter") despite first becoming aware of the Data Breach on or around November 11, 2021, over a year later.<sup>3</sup> During this time, Plaintiffs and Class Members were unaware that their sensitive PII had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm.

6. As a result of the Data Breach, criminal cyberthieves accessed and exfiltrated Plaintiffs' and Class Members' PII. The PII of at least 62,874 individuals was affected in the Data Breach.<sup>4</sup>

7. In its Notice Letter, Defendant does not explain the precise scope of the Data Breach or how long the unauthorized actor had access to Defendant's network.

---

hands (for example, Social Security numbers, passport numbers, driver's license numbers, financial account numbers).

<sup>2</sup> Office of the Maine Attorney General, <https://apps.web.maine.gov/online/aeviewer/ME/40/eef6c8d2-960c-4060-a0aa-511307fae33a/41c49cc4-9e77-41f5-a433-ad674b4be855/document.html> (last visited Feb. 10, 2023)

<sup>3</sup> See *Id.*

<sup>4</sup> Office of the Maine Attorney General, <https://apps.web.maine.gov/online/aeviewer/ME/40/eef6c8d2-960c-4060-a0aa-511307fae33a.shtml>

8. The Notice Letter provides no further information regarding the Data Breach and only goes on to recommend how victims can place a fraud alert or credit freeze on their account and how to sign up for the identity monitoring services Defendant offered in response to the Data Breach. The letters Plaintiffs and other Class Members received do not explain how the Data Breach occurred, what steps Defendant took following the Data Breach, whether Defendant made any changes to its data security, or most importantly, whether Plaintiffs' PII remains in the possession of criminals.

9. Defendant failed to reasonably store, secure, and monitor the PII it acquired and utilized as part of providing business services to its clients. As a result, Plaintiffs and Class Members suffered present injury and damages in the form of identity theft, loss of value of their PII, out-of-pocket expenses, and the loss of value of their time reasonably incurred to remedy or mitigate the effects of the unauthorized access, exfiltration, and subsequent criminal misuse of their sensitive and highly personal information.

10. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiffs and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion. Defendant's conduct in breaching these duties amounts to negligence and/or recklessness and violates federal and state statutes.

11. Plaintiffs bring this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to take reasonable steps to protect the PII of Plaintiffs and Class Members and Defendant's failure to warn Plaintiffs and Class Members of Defendant's inadequate information security practices. Defendant disregarded the rights of Plaintiffs and Class Members by knowingly failing to implement and maintain adequate and reasonable measures to ensure that the PII of Plaintiffs and Class Members was safeguarded, failing to take available steps to prevent

an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use.

12. As a direct and proximate result of Defendant's data security failures and the Data Breach, the PII of Plaintiffs and Class Members was compromised through disclosure to an unknown and unauthorized third party, and Plaintiffs and Class Members have suffered actual, present, concrete injuries. These injuries include: (i) the current and imminent risk of fraud and identity theft; (ii) lost or diminished value of PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iv) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (v) the continued and certainly increased risk to their PII, which remains unencrypted and available for unauthorized third parties to access and abuse and may remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII; (vi) the invasion of privacy; (vii) the compromise, disclosure, theft, and unauthorized use of Plaintiffs' and the Class Members' PII; and (viii) emotional distress, fear, anxiety, nuisance, and annoyance related to the theft and compromise of their PII.

13. Plaintiffs and Class Members seek to remedy these harms and prevent any future data compromise on behalf of themselves and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and remains at risk due to inadequate data security.

14. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

## II. PARTIES

### *Plaintiff Diane S. Jones*

15. Plaintiff Diane S. Jones is a resident and citizen of the state of Maryland, currently residing in Waldorf, Maryland. Plaintiff was notified of the Data Breach and of her PII being compromised via the Notice Letter, which she received directly from Defendant, dated January 13, 2023, by U.S. Mail. All of Plaintiff's claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

16. Plaintiff Joan Ogg is a resident and citizen of the state of New Hampshire, currently residing in Bow, New Hampshire. Plaintiff was notified of the Data Breach and of her PII being compromised via the Notice Letter, which she received directly from Defendant, dated December 19, 2022 by U.S. Mail. All of Plaintiff's claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

### *Defendant P2ES Holdings, LLC*

17. Defendant P2ES Holdings, LLC is a Delaware limited liability company with a principal place of business at 1670 Broadway, Suite 2800, Denver, Colorado 80202. Upon information and belief, members of P2ES Holdings, LLC include Mark Kilpatrick and J. Scott Lockhart of Colorado, Eric Wei of New York, and Chris Egan of Massachusetts.

18. All of Plaintiffs' claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

## III. JURISDICTION AND VENUE

19. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of \$5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class,

and at least one member of the class, including Plaintiff, are citizens of a state different from Defendant and its members.

20. This Court has personal jurisdiction over Defendant because its principal place of business is in this District and the acts and omissions giving rise to Plaintiffs' claims occurred in and emanated from this District.

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

#### **IV. FACTUAL ALLEGATIONS**

##### ***Defendant's Business***

22. Defendant P2 is a software and business services company based in Denver, Colorado that develops software for use in the oil and gas industry and offers a variety of services to oil and gas companies.

23. Defendant obtains the PII of Plaintiffs and Class Members in order to provide business services to its clients.

24. Plaintiffs and Class Members were consumers of Defendant or Defendant's business customers. Plaintiffs and Class Members were required to provide, and did in fact provide PII to Defendant in conjunction with obtaining services from Defendant or Defendant's business customers. Plaintiffs' and Class Members' PII were required to fill out various forms, including without limitation, applications, tax documents, accounting forms, various authorizations, and other form documents associated with the oil and gas industry.

25. Plaintiffs and Class Members relied on the sophistication of Defendant and its network to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class Members demand security to safeguard their PII.

26. Defendant required the submission of and voluntarily accepted the PII as part of its business and had a duty to adopt reasonable measures to protect the PII of Plaintiffs and Class Members from involuntary disclosure to third parties. Defendant has a legal duty to keep consumer PII safe and confidential.

27. The information held by Defendant in its computer systems and networks included the PII of Plaintiffs and Class Members.

28. On its customer-facing website, Defendant has a posted Privacy Policy, last updated May 2021 (the “Privacy Policy”) on its website.<sup>5</sup>

29. Defendant’s Privacy Policy acknowledges that Defendant has a duty to protect Plaintiffs’ and Class Members’ PII.

30. Defendant’s Privacy Policy pertains to PII provided to Defendant and any PII that Defendant collects.

31. The Privacy Policy “applies to all individuals whose personal information the Company collects, uses or discloses in the course of doing business. This includes individuals who are customers or potential customers who visit the Company’s website, and all individuals who are contract workers, contractors, and consultants to the Company. It is our policy to only disclose your personal information as required or authorized by law or as otherwise set out in this policy.”<sup>6</sup>

32. The Privacy Policy states “We will not use or share your information with anyone except as described in this Privacy Policy. When we receive information for our own purposes, such as the contact or billing information of our clients, the processing of that information is described by this privacy policy. When we receive or process information on behalf of one of our

---

<sup>5</sup> <https://www.p2energysolutions.com/privacypolicy> (last visited Feb. 10, 2023).

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

clients, the privacy practices that apply to the processing of that information are governed by our client’s privacy policy.”<sup>7</sup>

33. The Privacy Policy also provides, “We provide accounting software and associated services to the upstream oil and gas industry. In that capacity we receive personal information from our clients and process that information on behalf of our clients.”<sup>8</sup>

34. The Privacy Policy discusses the types of information Defendant collects and the reasons that it might use that information. It states, in part:

In addition to the specific situations discussed elsewhere in this policy, we disclose information in the following situations:

1. **Affiliates and Acquisitions.** We may share information with our corporate affiliates (*e.g.*, parent company, sister companies, subsidiaries, joint ventures, or other companies under common control). If another company acquires, or anticipates acquiring, our company, business, or our assets, we will also share information with that company.
2. **Other Disclosures with Your Consent.** We may ask if you would like us to share your information with other unaffiliated third parties who are not described elsewhere in this policy.
3. **Other Disclosures without Your Consent.** We may disclose information in response to subpoenas, warrants, or court orders, or in connection with any legal process, or to comply with relevant laws. We may also share your information in order to establish or exercise our rights, to defend against a legal claim, to investigate, prevent, or take action regarding possible illegal activities, suspected fraud, safety of person or property, or a violation of our policies, or to comply with your request for products to or the provision of services by a third-party intermediary.
4. **Service Providers.** We may share your information with service providers. Among other things service providers may help us to administer our website, conduct surveys, provide technical support, process payments, and assist in the fulfillment of orders.<sup>9</sup>

---

<sup>7</sup> *Id.*

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

<sup>9</sup> *Id.*



35. Defendant lists a number of instances when it might share or disclose the PII entrusted to it without permission, none of which are applicable to the Data Breach.

36. Defendant derived a substantial economic benefit from collecting Plaintiffs' and Class Members' PII.

37. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' PII from disclosure.

38. Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their PII. Defendant failed to implement industry standard protections for that sensitive information.

39. Plaintiffs and the Class Members relied on Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only and to make only authorized disclosures of this information.

***The Data Breach***

40. On or about November 11, 2021, Defendant "identified suspicious activity on certain computer systems in its network."<sup>10</sup>

41. On December 16, 2021, Defendant "received information that an unauthorized party may have accessed its network. P2 Energy commenced an investigation and cooperated with law enforcement."<sup>11</sup>

---

<sup>10</sup> <https://apps.web.maine.gov/online/aeviewer/ME/40/eef6c8d2-960c-4060-a0aa-511307fae33a.shtml> (Last visited Feb. 10, 2023).

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

42. On October 15, 2022, Defendant determined that one or more of the files contained the names and Social Security numbers of P2 consumers. Many of these customers, including Plaintiffs, were not notified until on or after January 13, 2023.<sup>12</sup>

43. Furthermore, Defendant's January 2023, notice letter states that an unauthorized party accessed and acquired certain files from its network between November 8, 2021, and November 17, 2021.<sup>13</sup>

44. To date, Defendant has not revealed the mechanism by which the unauthorized actor first gained access to its network.

45. However, upon information and belief, Defendant has no methods, policies, or procedures in place that would afford its consumers (like Plaintiffs and Class Members) any mechanism or opportunity to report misuse of the data back to Defendant, and the investigation commissioned by Defendant did not survey Defendant's clients whose data was breached for evidence of misuse.

46. The attacker accessed, copied, and acquired files on the server containing PII, including names and Social Security numbers.

47. Upon information and belief, the Data Breach occurred on certain networks that contained accounting related files.

48. On or around December 19, 2022, Defendant disclosed the Data Breach to the Maine Attorney General's Office.<sup>14</sup>

---

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

<sup>13</sup> *Id.*

<sup>14</sup> *Id.*

49. Defendant has disclosed that 62,874 individuals' PII was affected in the Data Breach.<sup>15</sup>

50. Plaintiffs' and Class Members' PII was accessed and stolen in the Data Breach

51. Defendant notified its impacted consumers of the incident as late as January 13, 2023, sending written notifications to individuals whose personal information was compromised in the Data Breach.

52. On information and belief, the PII accessed by hackers was not encrypted.

53. The targeted attack was expressly designed to gain access to and exfiltrate private and confidential data, including (among other things) the PII of Plaintiffs and the Class Members.

54. Due to Defendant's inadequate security measures, Plaintiffs and the Class Members now face a present, immediate, and ongoing risk of fraud and identity theft and must deal with that threat forever.

55. Due to Defendant's inadequate security measures, Plaintiffs' and Class Members' PII is now in the hands of cyberthieves.

56. Defendant failed to comply with its obligations to keep such information confidential and secure from unauthorized access.

***Defendant failed to comply with industry standards***

57. Defendant did not utilize industry standards appropriate to the nature of the sensitive, unencrypted information they were maintaining for Plaintiffs and Class Members, causing the exposure of PII.

---

<sup>15</sup> <https://apps.web.maine.gov/online/aevier/ME/40/eef6c8d2-960c-4060-a0aa-511307fae33a.shtml> (last visited Feb. 10, 2023).

58. As explained by the Federal Bureau of Investigation, “[p]revention is the most effective defense against cyberattacks] and it is critical to take precautions for protection.”<sup>16</sup>

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

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- 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.

---

<sup>16</sup> See How to Protect Your Networks from RANSOMWARE, at 3, available at <https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view> (last visited Feb. 10, 2023).

- 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>17</sup>

60. To prevent and detect cyber-attacks, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer.** Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks....
- **Use caution with links and when entering website addresses.** Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)....
- **Open email attachments with caution.** Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
- **Keep your personal information safe.** Check a website's security to ensure the information you submit is encrypted before you provide it....
- **Verify email senders.** If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.
- **Inform yourself.** Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known

---

<sup>17</sup> *How to Protect Your Networks from Ransomware*, available at: <https://www.justice.gov/criminal-ccips/file/872771/download> (last visited Feb. 2, 2023).

phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs.** Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic....<sup>18</sup>

61. To prevent and detect cyber-attacks 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;

**Build credential hygiene**

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

**Apply principle of least-privilege**

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

**Harden infrastructure**

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for

---

<sup>18</sup> *Security Tip (ST19-001) Protecting Against Ransomware* (original release date Apr. 11, 2019), available at: <https://us-cert.cisa.gov/ncas/tips/ST19-001> (last visited Feb. 2, 2023).

Office [Visual Basic for Applications].<sup>19</sup>

62. Given that Defendant was storing the PII of Plaintiffs and Class Members, Defendant could and should have implemented all of the above measures to prevent and detect cyber-attacks.

63. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent ransomware attacks, resulting in the Data Breach and the exposure of the PII of an undisclosed amount of current and former consumers, including Plaintiffs and Class Members.

***Defendant Acquires, Collects, and Stores the PII of Plaintiffs and Class Members***

64. Defendant acquires, collects, and stores the PII of Plaintiffs and Class Members as part of its business operations.

65. As part of utilizing the services Defendant's customers, Plaintiffs and Class Members, are required to provide, and did provide, their sensitive and confidential PII to Defendant's customers. Defendant acquires, retains, stores, processes, analyzes, and otherwise utilizes this information, and derives a substantial economic benefit from the PII that it collects. But for the collection of Plaintiffs' and Class Members' PII, Defendant would be unable to provide software and data solutions to the oil and gas industry.

66. By obtaining, collecting, and storing the PII of Plaintiffs and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the PII from disclosure.

67. Plaintiffs and Class Members have taken reasonable steps to maintain the

---

<sup>19</sup> *Human-operated ransomware attacks: A preventable disaster* (Mar 5, 2020), available at: <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/> (last visited Feb. 10, 2023).

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.

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

69. Defendant's policies on its website include promises and legal obligations to maintain and protect PII, demonstrating an understanding of the importance of securing PII.<sup>20</sup>

70. Defendant's negligence in safeguarding the PII of Plaintiffs and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

71. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiffs and Class Members from being compromised.

***The Data Breach was Foreseeable.***

72. Defendant knew and understood unprotected or exposed PII in the custody of manufacturing and distribution companies, such as Defendant, is valuable and highly sought after by nefarious third parties seeking to illegally monetize that PII through unauthorized access, as these companies maintain highly sensitive PII of consumers, including Social Security numbers and financial information.

73. In 2019, a record 1,473 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed, a 17% increase from 2018. The 525 reported breaches reported in 2019 exposed nearly 40 million sensitive records (39,378,157), compared to

---

<sup>20</sup> <https://www.p2energysolutions.com/privacypolicy> (last visited Feb. 10, 2023).



only 369 breaches that exposed just over 10 million sensitive records (10,632,600) in 2018.<sup>21</sup> These incidents continue to rise in frequency, with an estimated 1,862 data breaches occurring in 2021.<sup>22</sup>

74. In 2021 alone, there were over 220 data breach incidents.<sup>23</sup> These approximately 220 data breach incidents have impacted nearly 15 million individuals.<sup>24</sup>

75. Therefore, the increase in such attacks, and the attendant risk of future attacks, was widely known to the public and to anyone in Defendant’s industry, including Defendant.

***Value of Personally Identifiable Information***

76. The Federal Trade Commission (“FTC”) defines identity theft as “a fraud committed or attempted using the identifying information of another person without authority.”<sup>25</sup> The FTC describes “identifying information” as “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,” including, among other things, “[n]ame, Social Security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number.”<sup>26</sup>

77. The PII of individuals remains of high value to criminals, as evidenced by the prices the criminals will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, PII can be sold at a price ranging from \$40 to \$200, and bank

---

<sup>21</sup> *Id.* at p15.

<sup>22</sup> *Data breaches break record in 2021*, CNET, Jan. 24, 2022, available at: <https://www.cnet.com/news/privacy/record-number-of-data-breaches-reported-in-2021-new-report-says/> (last visited Feb. 10, 2023).

<sup>23</sup> *See* Kim Delmonico, *Another (!) Orthopedic Practice Reports Data Breach*, Orthopedics This Week (May 24, 2021), <https://ryortho.com/breaking/another-orthopedic-practice-reports-data-breach/> (last visited Feb. 10, 2023).

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

<sup>25</sup> 17 C.F.R. § 248.201 (2013).

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

details have a price range of \$50 to \$200.<sup>27</sup> Experian reports that a stolen credit or debit card number can sell for \$5 to \$110 on the dark web.<sup>28</sup> Criminals can also purchase access to entire company data breaches from \$900 to \$4,500.<sup>29</sup>

78. Social Security numbers, for example, are among the worst kind of PII to have stolen because Social Security numbers may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.<sup>30</sup>

79. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

---

<sup>27</sup> *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct. 16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last visited Feb. 10, 2023).

<sup>28</sup> *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, available at: <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> (last visited Feb. 10, 2023).

<sup>29</sup> *In the Dark*, VPNOverview, 2019, available at: <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/> (last visited Feb. 10, 2023).

<sup>30</sup> Social Security Administration, *Identity Theft and Your Social Security Number*, available at: <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last visited Feb. 10, 2023).

80. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, “[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number.”<sup>31</sup>

81. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to “close” and difficult, if not impossible, to change—one’s Social Security number.

82. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, “Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market.”<sup>32</sup>

83. Among other forms of fraud, identity thieves may use Social Security numbers to obtain driver’s licenses, government benefits, medical services, and housing or even give false information to police.

84. The fraudulent activity resulting from the Data Breach may not come to light for years.

85. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government

---

<sup>31</sup> Bryan Naylor, *Victims of Social Security Number Theft Find It’s Hard to Bounce Back*, NPR (Feb. 9, 2015), available at: <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft> (last visited Feb 10, 2023).

<sup>32</sup> Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card 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 Feb. 10, 2023).

Accountability Office (“GAO”), which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.<sup>33</sup>

86. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and Class Members, including Social Security numbers, and of the foreseeable consequences that would occur if Defendant’s data security system and network was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

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

88. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant’s server(s), amounting to potentially thousands of individuals’ detailed PII, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

89. In the Notice Letter, Defendant made an offer of twelve (12) months of credit and identity monitoring services. This is wholly inadequate to compensate Plaintiffs and Class Members as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiffs’ and Class Members’ PII.

---

<sup>33</sup> *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at: <https://www.gao.gov/assets/gao-07-737.pdf> (last visited Feb. 10, 2023).

90. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiffs and Class Members.

91. The ramifications of Defendant's failure to keep secure the PII of Plaintiffs and Class Members are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

***Defendant Violated the FTC Act***

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

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

***Plaintiff Diane S. Jones' Experience***

94. At the time of the Data Breach (November 8, 2021 to November 17, 2021), P2 retained Plaintiff Jones' PII in its system.

95. Plaintiff Jones greatly values her privacy and is very careful with her PII. Plaintiff Jones stores any documents containing PII in a safe and secure location or destroys such documents when they are no longer needed. Plaintiff Jones has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Moreover, Plaintiff Jones diligently

chooses unique usernames and passwords for her various online accounts. When Plaintiff Jones does entrust a third-party with her PII, it is only because she understands such information will be reasonably safeguarded from foreseeable threats, and that she will be timely notified if her data is exposed.

96. Plaintiff Jones provided PII, including her name and Social Security number, to one of Defendant's clients as a condition of receiving services. Upon information and belief, Defendant thereafter acquired this PII as part of its accounting operations.

97. Plaintiff Jones received a letter dated January 13, 2023, from Defendant notifying her of the Data Breach. The letter indicated that unauthorized third parties accessed and exfiltrated files on Defendant's server containing Plaintiff Jones' name and Social Security number.

98. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Jones faces, the letter offered Plaintiff Jones a twelve-month subscription to credit monitoring services. The letter further cautioned Plaintiff Jones to "remain vigilant against the possibility of fraud and identity theft by reviewing your financial account statements and credit reports for unauthorized activity ...."

99. Plaintiff contacted Defendant numerous times over the next several weeks regarding the scope and origin of the data breach to attempt to mitigate her damages. Despite Plaintiffs' requests, Defendant refused to disclose the identity of the third-party responsible for the Data Breach or whether Defendant or the third-party remained in possession of Plaintiffs' PII. Only after multiple telephone calls did Defendant even disclose to Plaintiff how Defendant first came into possession of Defendant's PII.

100. As a result of the Data Breach, Plaintiff Jones has spent several hours researching the Data Breach, verifying the legitimacy of the notice letter, utilizing credit monitoring services, reviewing her bank accounts, monitoring her credit report, changing her passwords and payment

account numbers, and other necessary mitigation efforts. This is valuable time Plaintiff Jones spent at Defendant's direction and that Plaintiff Jones otherwise would have spent on other activities, including but not limited to work and/or recreation.

101. The Data Breach caused Plaintiff Jones to suffer a loss of privacy.

102. As a result of the Data Breach, Plaintiff Jones will face a substantial risk of imminent harm for the rest of her life.

103. Plaintiff Jones anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the present and impending injuries caused by the Data Breach.

104. The substantial risk of harm and loss of privacy from the Data Breach has caused Plaintiff Jones to suffer fear, anxiety, annoyance, inconvenience, and nuisance. Plaintiff Jones was especially concerned that the Data Breach involved Defendant's accounting systems.

105. The Data Breach caused Plaintiff Jones to suffer a diminution in the value of her PII.

106. Plaintiff Jones has a continuing interest in ensuring that her PII, which upon information and belief, remains in Defendant's possession, is protected and safeguarded from future data breaches.

#### ***Plaintiff Joan Ogg's Experience***

107. Plaintiff Joan Ogg does not know how Defendant obtained her PII, and she had never heard of Defendant until she received the Notice Letter regarding the Data Breach in December 2022.

108. At the time of the Data Breach (November 8, 2021 to November 17, 2021), P2 retained Plaintiff Ogg's PII in its system.

109. Plaintiff Ogg is very careful about sharing her sensitive PII. Plaintiff Ogg stores any documents containing her PII in a safe and secure location. Plaintiff Ogg has never knowingly

transmitted unencrypted sensitive PII over the internet or any other unsecured source.

110. Plaintiff Ogg first learned of the Data Breach after receiving a data breach notification letter from P2, dated December 19, 2022, notifying her that Defendant suffered a data breach more than a year earlier and that her PII had been improperly accessed and/or obtained by unauthorized third parties while in possession of Defendant, including her name and Social Security number. Defendant's notice explained that Defendant came into possession of her PII because it "provides accounting and land management software to various customers in the oil and gas industry."

111. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, Plaintiff Ogg made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching the Data Breach; researching and signing up for the credit monitoring and identity theft protection services offered by Defendant; contacting credit bureaus to place credit freezes on her accounts; putting a block on her Social Security number through the IRS; contacting her trust account regarding fraudulent activity; and filing a police report in response to fraudulent activity. Plaintiff Ogg has spent several hours dealing with the Data Breach, valuable time Plaintiff Ogg otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

112. Plaintiff Ogg has suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to: (a) diminution in the value of her PII, a form of property that Defendant obtained from Plaintiff; (b) violation of her privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

113. The Data Breach has caused Plaintiff Ogg to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed her of key details about the Data Breach's occurrence.



114. As a result of the Data Breach, Plaintiff Ogg anticipates spending considerable time on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

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

116. Plaintiff Ogg has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

***Plaintiffs' and Class Members' Harms and Damages***

117. Defendant has done little to adequately protect Plaintiffs and Class Members, or to compensate them for their injuries sustained in the Data breach. Defendant's Notice Letter completely downplays and disavows the theft of Plaintiffs' and Class Members' PII when the facts demonstrate that the PII was accessed and exfiltrated. The complimentary fraud and identity monitoring service offered by Defendant is inadequate as the services are only offered for 12 months and require Plaintiffs and Class Members to expend time signing up.

118. Plaintiffs and Class Members have been injured and damaged by the compromise of their PII in the Data Breach.

119. Plaintiffs and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, tax return fraud, utility bills opened in their names, and similar identity theft.

120. Plaintiffs and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their PII as potential fraudsters could use that information to target such schemes more effectively to Plaintiffs and Class Members.

121. Plaintiffs and Class Members will also incur out-of-pocket costs for protective measures such as credit monitoring fees (for any credit monitoring obtained in addition to or in

lieu of the inadequate monitoring offered by Defendant), credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

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

123. Plaintiffs and Class Members were damaged from losing the benefit of their bargain. Plaintiffs and Class Members overpaid for a service that was intended to be accompanied by adequate data security but was not. Part of the price Plaintiffs and Class Members paid to Defendant and/or Defendant's clients was intended to be used by Defendant to fund adequate security of Defendant's computer property and protect Plaintiffs' and Class Members' PII. Thus, Plaintiffs and the Class Members did not get what they paid for.

124. Plaintiffs and Class Members have spent and will continue to spend significant amounts of time monitoring their financial accounts and records for misuse.

125. Plaintiffs and Class Members have and/or will suffer ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to: finding fraudulent loans, insurance claims, tax returns, and/or government benefit claims; purchasing credit monitoring and identity theft prevention; placing "freezes" and "alerts" with credit reporting agencies; spending time on the phone with or at a financial institution or government agency to dispute fraudulent charges and/or claims; contacting financial institutions and closing or modifying financial accounts; and closely reviewing and monitoring Social Security Number, bank accounts, and credit reports for unauthorized activity for the rest of their lives.

126. Plaintiffs and Class Members have an interest in ensuring that their PII, which is believed to remain in the possession of Defendant, is protected from further breaches by the

implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing sensitive and confidential personal, health, and/or financial information is not accessible online, that access to such data is password-protected, that such data is properly encrypted, and that such data is not stored for longer than Defendant has a legitimate need.

127. Further, as a result of Defendant's conduct, Plaintiffs and Class Members are forced to live with the anxiety that their PII may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

128. As a direct and proximate result of Defendant's actions and inactions, Plaintiffs and Class Members have suffered a loss of privacy and are at a present and imminent and increased risk of future harm.

## V. CLASS ALLEGATIONS

129. Plaintiffs bring this nationwide class action on themselves and on behalf of others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure. The nationwide Class that Plaintiffs seek to represent is defined as follows:

**All individuals residing in the United States whose PII was compromised in the data breach first announced by Defendant on or about December 19, 2022 (the "Class").**

130. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

131. Plaintiffs reserve the right to amend the definitions of the Class or add a Class or Subclass if further information and discovery indicate that the definitions of the Class should be

narrowed, expanded, or otherwise modified.

132. **Numerosity**, Fed R. Civ. P. 23(a)(1): The Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, at least multiple thousands of individuals were notified by Defendant of the Data Breach. According to the report submitted to the Maine Attorney's General office, 62,874 individuals had their PII compromised in this Data Breach.<sup>34</sup> The identities of Class Members are ascertainable through Defendant's records, Class Members' records, publication notice, self-identification, and other means.

133. **Commonality**, Fed. R. Civ. P. 23(a)(2) and (b)(3): There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

- a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' PII;
- b. 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;
- c. Whether Defendant data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
- d. Whether Defendant data security systems prior to and during the Data Breach were consistent with industry standards;
- e. Whether Defendant owed a duty to Class Members to safeguard their PII;
- f. Whether Defendant breached its duty to Class Members to safeguard their PII;

---

<sup>34</sup> See <https://apps.web.maine.gov/online/aeviewer/ME/40/eef6c8d2-960c-4060-a0aa-511307fae33a.shtml>

- g. Whether computer hackers obtained Class Members' PII in the Data Breach;
- h. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;
- i. Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;
- j. Whether Defendant's conduct was negligent;
- k. Whether Defendant's conduct was *per se* negligent, and;
- l. Whether Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

134. **Typicality**, Fed. R. Civ. P. 23(a)(3): Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' PII, like that of every other Class Member, was compromised in the Data Breach.

135. **Policies Generally Applicable to the Class**: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

136. **Adequacy of Representation**, Fed. R. Civ. P. 23(a)(4): Plaintiffs will fairly and adequately represent and protect the interests of Class Members. Plaintiffs' Counsel is competent and experienced in litigating Class actions, including data privacy litigation of this kind.

137. **Superiority and Manageability**, Fed. R. Civ. P. 23(b)(3): Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action

treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

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

139. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

140. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with

prosecuting this lawsuit as a class action.

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

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

143. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

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

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

145. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

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

146. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 145 above as if fully set forth herein.

147. Defendant collected and maintained the PII of Plaintiff and Class Members, who had no ability to influence or affect Defendant's data security policies.

148. Plaintiff and the Class Members, directly or indirectly, entrusted their PII to Defendant with the understanding that Defendant would safeguard their information.

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

150. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' PII held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

151. Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.



152. Defendant had a duty to employ reasonable security measures and otherwise protect the PII of Plaintiff and Class Members pursuant to Colo. Rev. Stat. § 6-1-713.5.

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

154. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' PII. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

- a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;
- b. Failing to adequately monitor the security of their networks and systems;
- c. Failing to periodically ensure that their email system had plans in place to maintain reasonable data security safeguards;
- d. Allowing unauthorized access to Class Members' PII; and,
- e. Failing to detect in a timely manner that Class Members' PII had been compromised.

155. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' PII would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the energy industry.

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

157. There is a temporal and close causal connection between Defendant's failure to implement security measures to protect the PII and the harm suffered, or risk of imminent harm suffered by Plaintiff and the Class.

158. As a result of Defendant's negligence, Plaintiff and the Class Members have suffered and will continue to suffer damages and injury including, but not limited to: increased risk of future identity theft and fraud, the costs associated therewith; time spent monitoring, addressing and correcting the current and future consequences of the Data Breach; and the necessity to engage legal counsel and incur attorneys' fees, costs and expenses.

159. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

160. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

**SECOND CAUSE OF ACTION**  
***Negligence Per Se***  
**(On Behalf of Plaintiffs and the Class)**

161. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 145 above as if fully set forth herein.

162. Pursuant to the Federal Trade Commission Act (15 U.S.C. § 45), Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII.

163. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as

Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

164. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect individuals' PII that it collected and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, and the foreseeable consequences of a data breach including, specifically, the damages that would result to Plaintiff and Class Members.

165. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se* as Defendant's violation of the FTC Act establishes the duty and breach elements of negligence.

166. Plaintiff and Class Members are within the class of persons that the FTC Act was intended to protect.

167. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

168. In addition, Defendant's conduct violated Colo. Rev. Stat. § 6-1-713.5. Colo. Rev. Stat. § 6-1-713.5 requires commercial entities who maintain, own, or license "personal identifying information of an individual residing in the state" to "implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal identifying information and the nature and size of the business and its operations."

169. Defendant failed to comply with Colo. Rev. Stat. § 6-1-713.5. Specifically, Defendant voluntarily undertook the act of maintaining and storing Plaintiff's PII but Defendant failed to implement safety and security procedures and practices sufficient enough to protect from the data breach that it should have anticipated. Defendant should have known and anticipated that

data breaches were on the rise, and that PII is a lucrative or likely target of cybercriminals looking to steal PII. Correspondingly, Defendant should have implemented and maintained procedures and practices appropriate to the nature and scope of information compromised in the data breach.

170. Plaintiff and Class Members are within the class of persons that Colo. Rev. Stat. § 6-1-713.5 was intended to protect.

171. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se*.

172. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

173. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that they were failing to meet their duties, and that Defendant's breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their PII.

174. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

**THIRD CAUSE OF ACTION**  
**Breach of Implied Contract**  
**(On Behalf of Plaintiffs and the Class)**

175. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 145 above as if fully set forth herein.

176. The PII of Plaintiffs and Class Members, including first and last name and Social Security numbers, was provided and entrusted to Defendant.

177. Plaintiffs and Class Members provided their PII to Defendant, either directly or indirectly through Defendant's clients, as part of Defendant's regular business practices.

178. As a condition of obtaining services from Defendant's clients, Plaintiffs and Class Members provided and entrusted their PII. In so doing, Plaintiffs and Class Members entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and Class Members if their data had been breached and compromised or stolen.

179. A meeting of the minds occurred when Plaintiffs and Class Members agreed to, and did, provide their PII to Defendant and/or Defendant's clients with the reasonable understanding that their PII would be adequately protected by any business associates, like Defendant, from foreseeable threats. This inherent understanding exists independent of any other law or contractual obligation any time that highly sensitive PII is exchanged as a condition of receiving services. It is common sense that but for this implicit and/or explicit agreement, Plaintiffs and Class Members would not have provided their PII.

180. Defendant separately has contractual obligations arising from and/or supported by the consumer facing statements in its Privacy Policy.

181. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Defendant.

182. Defendant breached the implied contracts it made with Plaintiffs and Class Members by failing to safeguard and protect their PII and by failing to provide timely and accurate notice that PII was compromised as a result of the Data Breach.

183. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiffs and Class Members have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of

the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

184. As a result of Defendant's breach of implied contract, Plaintiffs and Class Members are entitled to and demand actual, consequential, and nominal damages.

**FOURTH CAUSE OF ACTION**  
**Breach Of Third-Party Beneficiary Contract**  
**(On Behalf of Plaintiffs and the Class)**

185. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 145 above as if fully set forth herein.

186. Plaintiffs bring this claim for breach of third-party beneficiary contract against Defendants in the alternative to Plaintiffs' claim for breach of implied contract.

187. Defendants entered into various contracts with its oil and gas industry clients to provide business and accounting services to its clients.

188. These contracts are virtually identical to each other and were made expressly for the benefit of Plaintiffs and Class Members, as it was their confidential PII that Defendant agreed to collect and protect through its services. Thus, the benefit of collection and protection of the PII belonging to Plaintiffs and Class Members was the direct and primary objective of the contracting parties.

189. Defendant knew that if it were to breach these contracts with its oil and gas industry clients, the clients' customers, including Plaintiffs and Class Members, would be harmed by, among other things, fraudulent misuse of their PII.

190. Defendant breached its contracts with its clients when it failed to use reasonable data security measures that could have prevented the Data Breach and resulting compromise of Plaintiffs' and Class Members' PII.

191. As reasonably foreseeable, Plaintiffs and Class Members were harmed by Defendant's failure to use reasonable data security measures to store their PII, including but not limited to, the actual harm through the loss of their PII to cybercriminals.

192. Accordingly, Plaintiffs and Class Members are entitled to damages in an amount to be determined at trial, along with their costs and attorney fees incurred in this action.

**FIFTH CAUSE OF ACTION**  
**Breach Of Confidence**  
**(On Behalf of Plaintiffs and the Class)**

193. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 145 above as if fully set forth herein.

194. At all times during Defendant's possession of Plaintiffs' and the Class Members' PII, Defendant was fully aware of the confidential and sensitive nature of Plaintiffs' and the Class Members' PII.

195. Defendant's relationship with Plaintiffs and Class Members was governed by terms and expectations that Plaintiffs' and the Class Members' PII would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

196. Defendant voluntarily received in confidence Plaintiffs' and the Class Members' PII with the understanding that PII would not be disclosed or disseminated to the public or any unauthorized third parties.

197. Due to Defendant's failure to prevent and avoid the Data Breach from occurring, Plaintiffs' and the Class Members' PII was disclosed and misappropriated to unauthorized third

parties beyond Plaintiffs' and the Class Members' confidence, and without their express permission.

198. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiffs and Class Members have suffered damages.

199. But for Defendant's disclosure of Plaintiffs' and the Class Members' PII in violation of the parties' understanding of confidence, their PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiffs' and the Class Members' PII as well as the resulting damages.

200. The injury and harm Plaintiffs and Class Members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiffs' and the Class Members' PII. Defendant knew or should have known its methods of accepting and securing Plaintiffs' and the Class Members' PII was inadequate as it relates to, at the very least, securing servers and other equipment containing Plaintiffs' and the Class Members' PII.

201. As a direct and proximate result of Defendant's breach of its confidence with Plaintiffs and the Class, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual present and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendant's



possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of Plaintiffs and Class Members; and (viii) present and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

202. As a direct and proximate result of Defendant's breaches of confidence, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

**SIXTH CAUSE OF ACTION**  
**Unjust Enrichment**  
**(On Behalf of Plaintiffs and the Class)**

203. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 145 above as if fully set forth herein.

204. Defendant benefited from receiving Plaintiffs' and Class Members' PII by its ability to retain and use that information for its own benefit. Defendant understood this benefit.

205. Defendant also understood and appreciated that Plaintiffs' and Class Members' PII was private and confidential, and its value depended upon Defendant maintaining the privacy and confidentiality of that information.

206. Plaintiffs and Class Members conferred a monetary benefit upon Defendant in the form of purchasing services from Defendant, and in connection thereto, by providing their PII to Defendant with the understanding that Defendant would pay for the administrative costs of reasonable data privacy and security practices and procedures. Specifically, they were required to provide Defendant with their PII. In exchange, Plaintiffs and Class members should have received adequate protection and data security for such PII held by Defendant.

207. Defendant knew Plaintiffs and Class members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the PII of Plaintiffs and Class Members for business purposes.

208. Defendant enriched itself by saving the costs they reasonably should have expended to provide reasonable security, safeguards, and protections to the PII of Plaintiffs and Class Members.

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

210. Defendant wrongfully accepted and retained these benefits to the detriment of Plaintiffs and Class Members.

211. Defendant's enrichment at the expense of Plaintiffs and Class Members is and was unjust.

212. As a result of Defendant's wrongful conduct, as alleged above, Plaintiffs and the Class Members are entitled to restitution and disgorgement of all profits, benefits, and other compensation obtained by Defendant, plus attorneys' fees, costs, and interest thereon.

**SEVENTH CAUSE OF ACTION**  
**Violation of Colorado Consumer Protection Act,**  
**Colo. Rev. Stat. § 6-1-101, *et seq.***  
**(On behalf of Plaintiffs and the Class)**

213. Plaintiffs incorporate by reference all other allegations in the Complaint as if fully set forth herein.

214. The Colorado Consumer Protection Act, Colo. Rev. Stat. § 6-1-105(1)(l), *et seq.*, prohibits deceptive acts or practices in the conduct of any business, trade, or commerce, or in the furnishing of any service.

215. Defendant is a “person” under § 6-1-102(6) of the Colorado Consumer Protection Act (“Colorado CPA”), Colo. Rev. Stat. § 6-1-101, et seq.

216. Plaintiffs and Class Members provided and/or entrusted sensitive and confidential PII to Defendant, which Defendant collected, stored, and maintained at its Colorado headquarters.

217. Defendant is engaged in, and its acts and omissions affect, trade and commerce. Defendant’s relevant acts, practices and omissions complained of in this action were done in the course of Defendant’s business of marketing, offering for sale, and selling goods and services throughout the United States.

218. In the conduct of its business, trade, and commerce, Defendant engaged in the conduct alleged in this Complaint in transactions intended to result, and which did result, in the provision or sale of services to consumers. Plaintiffs and Class Members furnished or purchased these services. Plaintiffs and the Class Members are actual or potential consumers as defined by Colo. Rev. Stat § 6-1-113(1), et seq.

219. In the conduct of its business, trade, and commerce, Defendant collected and stored highly personal and PII, including PII belonging to Plaintiffs and Class Members.

220. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard the PII of Plaintiffs and the Class Members and that the risk of a data breach was highly likely and/or that the risk of the data breach being more extensive than originally disclosed was highly likely.

221. Defendant should have disclosed this information regarding its computer systems and data security practices because Defendant was in a superior position to know the true facts related to their security practices, and Plaintiffs and Class Members could not reasonably be expected to learn or discover the true facts.

222. As alleged herein this Complaint, Defendant engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce and the furnishing of customer relation services to consumers in violation of the Colorado CPA, including but not limited to the following:

- a. failing to adequately secure consumer's names and Social Security numbers;
- b. failing to maintain adequate computer systems and data security practices to safeguard consumers' PII;
- c. failing to disclose the material information, known at the time of the transaction—collection and retention of consumer PII to furnish customer relation services—that its computer systems would not adequately protect and safeguard consumer PII;
- d. inducing consumers to use Defendant's services by failing to disclose, and misrepresenting the material fact that, Defendant's computer systems and data security practices were inadequate to safeguard employee's and client's sensitive personal information from theft.

223. By engaging in the conduct delineated above, Defendant has violated the Colorado CPA by, among other things:

- a. omitting material facts regarding the goods and services sold;
- b. omitting material facts regarding the security of the transactions between Defendant and consumers;
- c. omitting material facts regarding the security of the transactions between Defendant and consumers who furnished or entrusted their PII;
- d. misrepresenting material facts in the furnishing or sale of products, goods or services to consumers;

- e. engaging in conduct that is likely to mislead consumers acting reasonably under the circumstances;
- f. engaging in conduct which creates a likelihood of confusion or of misunderstanding;
- g. engaging in conduct with the intent to induce consumers to use Defendant's service;
- h. unfair practices that caused or were likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers; and/or
- i. other unfair, deceptive, unconscionable, fraudulent and/or unlawful acts or practices to be shown at trial.

224. Defendant systemically engaged in these deceptive, misleading, and unlawful acts and practices, to the detriment of Plaintiffs and Class Members.

225. Defendant's actions in engaging in the conduct delineated above were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiffs and Class Members.

226. As a direct result of Defendant's violation of the Colorado Consumer Protection Act, Plaintiffs and the Class Members have suffered actual damages, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and

identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect that PII; and (viii) present and future costs in terms of time, effort, and money that has been and will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

227. As a result of Defendant's violation of the Colorado Consumer Protection Action, Plaintiffs and the Class Members are entitled to, and seek, injunctive relief, including, but not limited to:

- a. Ordering that Defendant engage third-party security auditors/penetration testers as well as experienced and qualified internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
- b. Ordering that Defendant engage third-party security auditors and experienced and qualified internal security personnel to run automated security monitoring;
- c. Ordering that Defendant audit, test, and train its security personnel regarding new or modified procedures;
- d. Ordering that Defendant's segment data by, among other things, creating firewalls and access controls so that if one area of Defendant is compromised, hackers cannot gain access to other portions of Defendant's systems;
- e. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner employee and customer data not necessary for its provision of services;
- f. Ordering that Defendant conduct regular database scanning and securing checks;

- g. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and,
- h. Ordering Defendant to meaningfully educate its employees and customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps customers must take to protect themselves.

228. As a direct and proximate result of the unconscionable, unfair, and deceptive acts or practices of Defendant alleged herein, Plaintiffs and the Class Members seek relief under Colo. Rev. Stat. § 6-1-113, including, but not limited to, the greater of actual damages, statutory damages, or treble damages for bad faith conduct, injunctive relief, attorneys' fees and costs, as allowable by law.

### **PRAYER FOR RELIEF**

**WHEREFORE**, Plaintiffs, individually, and on behalf of Class Members, request judgment against Defendant and that the Court grant the following:

- A. For an order certifying the Class, as defined herein, and appointing Plaintiff and her Counsel to represent the Class;
- B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiffs and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiffs and Class Members;
- C. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:

- i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;
- ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;
- iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiffs and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;
- iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiffs and Class Members;
- v. prohibiting Defendant from maintaining the PII of Plaintiffs and Class Members on a cloud-based database;
- vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
- vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;
- viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;
- ix. requiring Defendant to segment data by, among other things, creating firewalls



and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

- 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 Plaintiffs 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;
- xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;
- xv. requiring Defendant to meaningfully educate all Class Members about the

- threats that they face as a result of the loss of their confidential PII to third parties, as well as the steps affected individuals must take to protect themselves;
- xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;
- D. For an award of damages, including actual, statutory, nominal, and consequential damages, as allowed by law in an amount to be determined;
- E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;
- F. For prejudgment interest on all amounts awarded; and
- G. Such other and further relief as this Court may deem just and proper.

**DEMAND FOR JURY TRIAL**

Plaintiffs hereby demand that this matter be tried before a jury.

Dated: August 10, 2023

Respectfully submitted,

/s/ Terence R. Coates

**Terence R. Coates**

**Justin C. Walker \***

**Dylan J. Gould \***

MARKOVITS, STOCK & DEMARCO, LLC

119 E. Court Street, Suite 530

Cincinnati, OH 45202

Tel: 513.651-3700

E-mail: tcoates@msdlegal.com

jwalker@msdlegal.com

dgould@msdlegal.com

**Gary M. Klinger**

MILBERG COLEMAN BRYSON  
PHILLIPS GROSSMAN PLLC  
227 W. Monroe Street, Suite 2100  
Chicago, IL 60606  
Phone: (866) 252-0878  
E-mail: gklinger@milberg.com

**David K. Lietz**  
MILBERG COLEMAN BRYSON  
PHILLIPS GROSSMAN PLLC  
5335 Wisconsin Avenue NW, Suite 440  
Washington, D.C. 20015-2052  
E-mail: dlietz@milberg.com

*Attorneys for Plaintiffs and the Proposed Class*

*\*Admission Forthcoming*

**CERTIFICATE OF SERVICE**

I certify that on August 10, 2023, I electronically filed the foregoing using the Court's CM/ECF system, and served the same upon counsel for Defendant by electronic mail.

*/s/ Terence R. Coates* \_\_\_\_\_