IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO

Civil Action No. _____

DIANE S. JONES, on behalf of herself and all others similary situated,

Plaintiff,

v.

P2ES HOLDINGS, LLC dba P2 ENERGY SOLUTIONS,

Defendant.

CLASS ACTION COMPLAINT AND JURY TRIAL DEMAND

Plaintiff Diane S. Jones ("Plaintiff") brings this Class Action Complaint against P2ES Holdings, LLC dba P2 Energy Solutions ("Defendant" or "P2"), in her individual capacity and on behalf of all others similarly situated, and alleges, upon personal knowledge as to her own actions and her 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").

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 in Denver, Colorado.

3. Defendant acquires, processes, analyzes, and otherwise utilizes Plaintiff's 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 a through its subsequent investigation Defendant learned that an unauthorized party accessed and acquired certain files from its network.[1]

5. Defendant did not notify Plaintiff and Class Members until on or around January 13, 2023 ("Notice of Data Breach" or "Notice Letter") despite first becoming aware of the Data Breach on or around November 11, 2021, over a year later.[2] During this time, Plaintiff and Class Members were unaware that their sensitive PII had been compromised, and that they were, and continue to be, at present and significantly increased 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 Plaintiff's and Class Members' PII. The PII of at least 62,874 individuals was affected in the Data Breach.[3]

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.

8. The Notice Letter provides no further information regarding the Data Breach and

[1] 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).
[2] See *Id.*
[3] Office of the Maine Attorney General, https://apps.web.maine.gov/online/aeviewer/ME/40/eef6c8d2-960c-4060-a0aa-511307fae33a.shtml

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 Plaintiff 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 Plaintiff's 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, Plaintiff 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 Plaintiff 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. Plaintiff brings 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 Plaintiff and Class Members and Defendant's failure to warn Plaintiff and Class Members of Defendant's inadequate information security practices. Defendant disregarded the rights of Plaintiff and Class Members by knowingly failing to implement and maintain adequate and reasonable measures to ensure that the PII of Plaintiff 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 Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party, and Plaintiff 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 Plaintiff's and the Class Members' PII; and (viii) emotional distress, fear, anxiety, nuisance, and annoyance related to the theft and compromise of their PII.

13. Plaintiff 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. Plaintiff 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, and at all times relevant has been, a resident and citizen of Maryland, residing in Waldorf, Maryland, where she intends to remain. Plaintiff received a data breach notice letter from Defendant, dated January 13, 2023, by U.S. Mail.

Defendant P2ES Holdings, LLC

16. Defendant P2ES Holdings, LLC is a Delaware limited liability company with a principal place of business at 1670 Broadway, Suite 2800, Denver, Colorado 80202. Members of P2ES Holdings, LLC include Mark Kilpatrick and J. Scott Lockhart who are citizens of Colorado, Eric Wei who is a citizen of New York, and Chris Egan who is a citizen of Massachusetts.

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

III. JURISDICTION AND VENUE

18. 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, is a citizen of a state different from Defendant and its members.

19. 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 Plaintiff's claims occurred in and emanated from this District.

20. 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

21. 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.

22. Defendant obtains the Plaintiff's and Class Members' PII in order to provide business services to its clients.

23. Plaintiff and Class Members were consumers of Defendant or Defendant's business customers. Plaintiff 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. Plaintiff's 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.

24. Plaintiff 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. Plaintiff and Class Members demand security to safeguard their PII.

25. 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 Plaintiff and Class Members from involuntary disclosure to third parties. Defendant has a legal duty to keep consumer PII safe and confidential.

26. The information held by Defendant in its computer systems and networks included Plaintiff and Class Members' PII.

27. On its customer-facing website, Defendant has a posted Privacy Policy, last updated May 2021 (the "Privacy Policy") on its website.

28. Defendant's Privacy Policy acknowledges that Defendant has a duty to protect Plaintiff's and Class Members' PII.

29. Defendant's Privacy Policy pertains to PII provided to Defendant and any PII that Defendant collects.

30. 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."[4]

31. 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 clients, the privacy practices that apply to the processing of that information are governed by our client's privacy policy."[5]

32. 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."[6]

[4] https://www.p2energysolutions.com/privacypolicy (last visited Feb. 10, 2023).
[5] *Id.*
[6] *Id.*

33. 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.[7]

34. 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.

35. Defendant derived a substantial economic benefit from collecting Plaintiff's and Class Members' PII.

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

---

[7] *Id.*

37. Plaintiff 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.

38. Plaintiff 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

39. On or about November 11, 2021, Defendant "identified suspicious activity on certain computer systems in its network."[8]

40. 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." [9]

41. 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 individuals, including Plaintiff, were not notified until January 13, 2023.[10]

42. Furthermore, Defendant's Notice Letter states that an unauthorized party accessed and acquired certain files from its network between November 8, 2021, and November 17, 2021.[11]

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

44. However, upon information and belief, Defendant has no methods, policies, or

[8] https://apps.web.maine.gov/online/aeviewer/ME/40/eef6c8d2-960c-4060-a0aa-511307fae33a.shtml (Last visited Feb. 10, 2023).
[9] *Id.*
[10] *Id.*
[11] *Id.*

procedures in place that would afford its consumers (like Plaintiff 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.

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

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

47. On or around December 19, 2022, Defendant disclosed the Data Breach to the Maine Attorney General's Office.[12]

48. Defendant has disclosed that 62,874 individuals' PII was affected in the Data Breach.[13]

49. Plaintiff's and Class Members' PII was accessed and stolen in the Data Breach.

50. 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.

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

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

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

[12] *Id.*

[13] https://apps.web.maine.gov/online/aeviewer/ME/40/eef6c8d2-960c-4060-a0aa-511307fae33a.shtml (last visited Feb. 10, 2023).

threat forever.

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

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

Defendant failed to comply with industry standards

56. Defendant did not utilize industry standards appropriate to the nature of the sensitive, unencrypted information they were maintaining for Plaintiff and Class Members, causing the exposure of PII for more than 62,000 individuals.

57. 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."[14]

58. 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.

[14] *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).

- 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.
- 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.[15]

59. 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

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

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 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….[16]

60. 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

[16] *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).

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 Office [Visual Basic for Applications].[17]

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

62. 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 Plaintiff and Class Members.

[17] *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).

Defendant Acquires, Collects, and Stores the PII of Plaintiff and Class Members

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

64. As part of utilizing the services Defendant's customers, Plaintiff 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 Plaintiff's and Class Members' PII, Defendant would be unable to provide software and data solutions to the oil and gas industry.

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

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

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

68. 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.[18]

69. Defendant's negligence in safeguarding the PII of Plaintiff and Class Members is

[18] https://www.p2energysolutions.com/privacypolicy (last visited Feb. 10, 2023).

exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

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

The Data Breach was Foreseeable.

71. 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.

72. 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 only 369 breaches that exposed just over 10 million sensitive records (10,632,600) in 2018.19 These incidents continue to rise in frequency, with an estimated 1,862 data breaches occurring in 2021.[20]

73. In 2021 alone, there were over 220 data breach incidents.[21] These approximately 220 data breach incidents impacted nearly 15 million individuals.[22]

---

[19] *Id.* at 15.

[20] *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).

[21] *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).

[22] *Id*.

74. 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

75. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[23] 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."[24]

76. 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 details have a price range of $50 to $200.[25] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[26] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[27]

77. Social Security numbers, for example, are among the worst kind of PII to have

---

[23] 17 C.F.R. § 248.201 (2013).
[24] *Id*.
[25] *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).
[26] *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).
[27] *In the Dark*, VPNOverview, 2019, available at: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Feb. 10, 2023).

stolen because they 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.[28]

78. 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.

79. 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."[29]

80. 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

---

[28] 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).

[29] 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).

compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—one's Social Security number.

81. 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."[30]

82. 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.

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

84. 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 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.[31]

85. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members, including Social Security numbers, and of the foreseeable consequences that would occur if Defendant's data security

---

[30] 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).

[31] *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).

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

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

87. 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.

88. In the breach notification letter, Defendant made an offer of twelve (12) months of credit and identity monitoring services. This is wholly inadequate to compensate Plaintiff 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 Plaintiff's and Class Members' PII.

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

90. The ramifications of Defendant's failure to keep secure the PII of Plaintiff 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

91. 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.

92. 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 Plaintiff and Class Members.

Plaintiff Diane S. Jones' Experience

93. 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.

94. 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.

95. 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.

96. 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 …."

97. 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 Plaintiff's 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 Plaintiff's PII. Only after multiple telephone calls did Defendant even disclose to Plaintiff how Defendant first came into possession of Plaintiff's PII.

98. As a result of the Data Breach, Plaintiff Jones has spent approximately 10 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.

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

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

101. 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.

102. 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 is especially concerned that the Data Breach involved Defendant's accounting systems.

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

104. 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's and Class Members' Harms and Damages

105. Defendant has done little to adequately protect Plaintiff and Class Members, or to compensate them for their injuries sustained in the Data breach. Defendant's Notice of Data Breach completely downplays and disavows the theft of Plaintiff's 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 Plaintiff and Class Members to expend time signing up for it.

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

107. Plaintiff 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.

108. Plaintiff 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 Plaintiff and Class Members.

109. Plaintiff 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.

110. Plaintiff 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.

111. Plaintiff and Class Members were damaged from losing the benefit of their bargain. Plaintiff and Class Members overpaid for a service that was intended to be accompanied by adequate data security but was not. Part of the price Plaintiff 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 Plaintiff's and Class Members' PII. Thus, Plaintiff and the Class Members did not get what they paid for.

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

113. Plaintiff 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 years to come.

114. Plaintiff 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.

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

116. As a direct and proximate result of Defendant's actions and inactions, Plaintiff 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

117. Plaintiff bring this nationwide class action on behalf of herself 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 Plaintiff seek to represent is defined as follows:

> **All persons P2 identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach.**

118. Excluded from the Classes 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.

119. Plaintiff reserves the right to modify or amend the definition of the proposed class and any future subclass before the Court determines whether certification is appropriate.

120. **Numerosity,** Fed R. Civ. P. 23(a)(1): The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, reports indicate that approximately 62,874 individuals had their PII compromised in this Data Breach. The identities of Class Members are ascertainable through Defendant's records, Class Members' records, publication notice, self-identification, and other means.

121. **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 Plaintiff's 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;

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

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

123. **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 Plaintiff's 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 Plaintiff.

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

125. **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.

126. 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.

127. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff 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 Plaintiff 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.

128. 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.

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

130. Unless a Class-wide injunction is issued, Defendant may continue in its 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.

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

132. 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 Plaintiff 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.

133. 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 Plaintiff and the Class)

134. Plaintiff incorporates by reference all other allegations in the Complaint as if fully set forth herein.

135. Plaintiff and the Class entrusted Defendant with their PII.

136. Plaintiff and the Class entrusted their PII to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

137. Defendant has 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.

138. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII of Plaintiff and Class Members involved an unreasonable risk of harm to Plaintiff and Class Members, even if the harm occurred through the criminal acts of a third-party.

139. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing

Defendant's security protocols to ensure that the PII of Plaintiff and Class Members in Defendant's possession was adequately secured and protected.

140. Defendant also had a duty to exercise appropriate clearinghouse practices to remove PII they were no longer required to retain pursuant to regulations.

141. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII of Plaintiff and the Class.

142. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential PII, a necessary part of obtaining services from Defendant. That duty further arose because Defendant chose to collect and maintain the PII for its own pecuniary benefit.

143. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or the Class.

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

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

146. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and the Class. Defendant's misconduct included, but was not limited to, its failure to take the steps and

opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decisions not to comply with industry standards for the safekeeping of the PII of Plaintiff and the Class, including basic encryption techniques freely available to Defendant.

147. Plaintiff and the Class had no ability to protect their PII that was in, and possibly remains in, Defendant's possession.

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

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

150. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiff and the Class.

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

152. Defendant, through their actions and/or omissions, unlawfully breached their duties to Plaintiff and the Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiff and the Class during the time the PII was within Defendant's possession or control.

153. Defendant improperly and inadequately safeguarded the PII of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

154. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the PII of Plaintiff and the Class in the face of increased risk of theft.

155. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and the Class by failing to have appropriate procedures in place to detect and prevent dissemination of PII.

156. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove PII they were no longer required to retain pursuant to regulations.

157. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and the Class the existence and scope of the Data Breach.

158. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Nationwide Class, the PII of Plaintiff and the Class would not have been compromised.

159. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiff and the Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Nationwide Class. The PII of Plaintiff and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

160. Additionally, 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.

161. 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 Plaintiff and the Class.

162. Defendant's violation of Section 5 of the FTC Act constitutes negligence per se.

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

164. 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.

165. As a direct and proximate result of Defendant's negligence and negligence per se, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (if) actual identity theft; (ii) the loss of the opportunity of 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 continuing 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 Plaintiff and the Class; and (viii) present and continuing 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 Plaintiff and the Class.

166. As a direct and proximate result of Defendant's negligence and negligence per se, Plaintiff and the Class 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.

167. Additionally, as a direct and proximate result of Defendant's negligence and negligence per se, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of 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 in its continued possession.

168. As a direct and proximate result of Defendant's negligence and negligence per se, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages.

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

169. Plaintiff incorporates by reference all other allegations in the Complaint as if fully set forth herein.

170. The PII of Plaintiff and the Class, including first and last name and Social Security numbers, was provided and entrusted to Defendant.

171. Plaintiff and the Class provided their PII to Defendant, either directly or indirectly through Defendant's clients, as part of Defendant's regular business practices.

172. As a condition of obtaining services from Defendant's clients, Plaintiff and the Class provided and entrusted their PII. In so doing, Plaintiff and the Class 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 Plaintiff and the Class if their data had been breached and compromised or stolen.

173. A meeting of the minds occurred when Plaintiff and the Class 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, Plaintiff and Class Members would not have provided their PII.

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

175. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendant.

176. Defendant breached the implied contracts it made with Plaintiff and the Class 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.

177. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class 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.

178. As a result of Defendant's breach of implied contract, Plaintiff and the Class are entitled to and demand actual, consequential, and nominal damages.

THIRD CAUSE OF ACTION
Breach Of Confidence
(On Behalf of Plaintiff and the Class)

179. Plaintiff incorporates by reference all other allegations in the Complaint as if fully set forth herein.

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

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

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

183. Due to Defendant's failure to prevent and avoid the Data Breach from occurring, Plaintiff's and the Class Members' PII was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and the Class Members' confidence, and without their express permission.

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

185. But for Defendant's disclosure of Plaintiff's 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 Plaintiff's and the Class Members' PII as well as the resulting damages.

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

187. As a direct and proximate result of Defendant's breach of its confidence with Plaintiff and the Class, Plaintiff 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 Plaintiff and the Class; 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 Plaintiff and the Class.

188. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff 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.

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

189. Plaintiff incorporates by reference all other allegations in the Complaint as if fully set forth herein.

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

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

192. Plaintiff 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, Plaintiff and Class members should have received adequate protection and data security for such PII held by Defendant.

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

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

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

196. Defendant wrongfully accepted and retained these benefits to the detriment of Plaintiff and Class Members.

197. Defendant's enrichment at the expense of Plaintiff and Class Members is and was unjust.

198. As a result of Defendant's wrongful conduct, as alleged above, Plaintiff 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.

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

199. Plaintiff incorporates by reference all other allegations in the Complaint as if fully set forth herein.

200. 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.

201. 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.

202. Plaintiff and the Class provided and/or entrusted sensitive and confidential PII to Defendant, which Defendant collected, stored, and maintained at its Colorado headquarters.

203. 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.

204. 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. Plaintiff and other members of the Class furnished or purchased these services. Plaintiff and the Class Members are actual or potential consumers as defined by Colo. Rev. Stat § 6-1-113(1), et seq.

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

206. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard the PII of Plaintiff 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.

207. 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 Plaintiff and the Class Members could not reasonably be expected to learn or discover the true facts.

208. 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.

209. By engaging in the conduct delineated above, Defendant has violated the Colorado Consumer Protection Act 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.

210. Defendant systemically engaged in these deceptive, misleading, and unlawful acts and practices, to the detriment of Plaintiff and the Class.

211. 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 Plaintiff and the Class.

212. As a direct result of Defendant's violation of the Colorado Consumer Protection Act, Plaintiff 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 Plaintiff and the Nationwide Class.

213. As a result of Defendant's violation of the Colorado Consumer Protection Action, Plaintiff 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.

214. As a direct and proximate result of the unconscionable, unfair, and deceptive acts or practices of Defendant alleged herein, Plaintiff 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, Plaintiff, on behalf of herself and Class Members, requests 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 each such 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 Plaintiff and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff 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 Plaintiff 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 Plaintiff 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 Plaintiff and Class Members;

v. prohibiting Defendant from maintaining the PII of Plaintiff 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 Plaintiff and Class Members;

xii. requiring Defendant to conduct internal training and education routinely and continually, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its employees' knowledge of the education programs discussed in the preceding

subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

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

Plaintiff hereby demands that this matter be tried before a jury.

Dated: February 12, 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

Attorneys for Plaintiff and the putative Class

**To be Admitted Pro Hac Vice*

JS 44 (Rev. 11/15) District of Colorado Form

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

Diane S. Jones

(b) County of Residence of First Listed Plaintiff Charles County
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Terence R. Coates, Justin C. Walker, Dylan J. Gould, Markovits, Stock & DeMarco, LLC, 119 E. Court St., Suite 530, Cincinnati, OH 45202; Phone: (513) 651-3700

DEFENDANTS

P2ES Holdings, LLC dba P2 Energy Solutions

County of Residence of First Listed Defendant Denver
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ❒ 1 U.S. Government Plaintiff
- ❒ 3 Federal Question *(U.S. Government Not a Party)*
- ❒ 2 U.S. Government Defendant
- ☒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*
(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	❒ 1	❒ 1	Incorporated *or* Principal Place of Business In This State	❒ 4	☒ 4
Citizen of Another State	☒ 2	❒ 2	Incorporated *and* Principal Place of Business In Another State	❒ 5	❒ 5
Citizen or Subject of a Foreign Country	❒ 3	❒ 3	Foreign Nation	❒ 6	❒ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

CONTRACT
- ❒ 110 Insurance
- ❒ 120 Marine
- ❒ 130 Miller Act
- ❒ 140 Negotiable Instrument
- ❒ 150 Recovery of Overpayment & Enforcement of Judgment
- ❒ 151 Medicare Act
- ❒ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ❒ 153 Recovery of Overpayment of Veteran's Benefits
- ❒ 160 Stockholders' Suits
- ☒ 190 Other Contract
- ❒ 195 Contract Product Liability
- ❒ 196 Franchise

REAL PROPERTY
- ❒ 210 Land Condemnation
- ❒ 220 Foreclosure
- ❒ 230 Rent Lease & Ejectment
- ❒ 240 Torts to Land
- ❒ 245 Tort Product Liability
- ❒ 290 All Other Real Property

TORTS

PERSONAL INJURY
- ❒ 310 Airplane
- ❒ 315 Airplane Product Liability
- ❒ 320 Assault, Libel & Slander
- ❒ 330 Federal Employers' Liability
- ❒ 340 Marine
- ❒ 345 Marine Product Liability
- ❒ 350 Motor Vehicle
- ❒ 355 Motor Vehicle Product Liability
- ❒ 360 Other Personal Injury
- ❒ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ❒ 365 Personal Injury - Product Liability
- ❒ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ❒ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ❒ 370 Other Fraud
- ❒ 371 Truth in Lending
- ❒ 380 Other Personal Property Damage
- ❒ 385 Property Damage Product Liability

CIVIL RIGHTS
- ❒ 440 Other Civil Rights
- ❒ 441 Voting
- ❒ 442 Employment
- ❒ 443 Housing/ Accommodations
- ❒ 445 Amer. w/Disabilities - Employment
- ❒ 446 Amer. w/Disabilities - Other
- ❒ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ❒ 463 Alien Detainee
- ❒ 510 Motions to Vacate Sentence
- ❒ 530 General
- ❒ 535 Death Penalty

Other:
- ❒ 540 Mandamus & Other
- ❒ 550 Civil Rights
- ❒ 555 Prison Condition
- ❒ 560 Civil Detainee - Conditions of Confinement

FORFEITURE/PENALTY
- ❒ 625 Drug Related Seizure of Property 21 USC 881
- ❒ 690 Other

LABOR
- ❒ 710 Fair Labor Standards Act
- ❒ 720 Labor/Management Relations
- ❒ 740 Railway Labor Act
- ❒ 751 Family and Medical Leave Act
- ❒ 790 Other Labor Litigation
- ❒ 791 Employee Retirement Income Security Act

IMMIGRATION
- ❒ 462 Naturalization Application
- ❒ 465 Other Immigration Actions

BANKRUPTCY
- ❒ 422 Appeal 28 USC 158
- ❒ 423 Withdrawal 28 USC 157

PROPERTY RIGHTS
- ❒ 820 Copyrights
- ❒ 830 Patent
- ❒ 840 Trademark

SOCIAL SECURITY
- ❒ 861 HIA (1395ff)
- ❒ 862 Black Lung (923)
- ❒ 863 DIWC/DIWW (405(g))
- ❒ 864 SSID Title XVI
- ❒ 865 RSI (405(g))

FEDERAL TAX SUITS
- ❒ 870 Taxes (U.S. Plaintiff or Defendant)
- ❒ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
- ❒ 375 False Claims Act
- ❒ 376 Qui Tam (31 USC 3729(a))
- ❒ 400 State Reapportionment
- ❒ 410 Antitrust
- ❒ 430 Banks and Banking
- ❒ 450 Commerce
- ❒ 460 Deportation
- ❒ 470 Racketeer Influenced and Corrupt Organizations
- ❒ 480 Consumer Credit
- ❒ 490 Cable/Sat TV
- ❒ 850 Securities/Commodities/ Exchange
- ❒ 890 Other Statutory Actions
- ❒ 891 Agricultural Acts
- ❒ 893 Environmental Matters
- ❒ 895 Freedom of Information Act
- ❒ 896 Arbitration
- ❒ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ❒ 950 Constitutionality of State Statutes

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ❒ 2 Removed from State Court ❒ 3 Remanded from Appellate Court ❒ 4 Reinstated or Reopened ❒ 5 Transferred from Another District *(specify)* ❒ 6 Multidistrict Litigation

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
28 U.S.C. 1332(d)

Brief description of cause:
Defendant failed to protect Plaintiff's private information

❒ AP Docket

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.

DEMAND $ 5,000,001.00

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ❒ No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE _____ DOCKET NUMBER _____

DATE
02/12/2023

SIGNATURE OF ATTORNEY OF RECORD
/s/ Terence R. Coates

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

I.(a) **Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

(b) **County of Residence.** For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

(c) **Attorneys.** Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".

II. **Jurisdiction.** The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.
United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below**; NOTE: federal question actions take precedence over diversity cases.**)

III. **Residence (citizenship) of Principal Parties.** This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. **Nature of Suit.** Place an "X" in the appropriate box. If the nature of suit cannot be determined, be sure the cause of action, in Section VI below, is sufficient to enable the deputy clerk or the statistical clerk(s) in the Administrative Office to determine the nature of suit. If the cause fits more than one nature of suit, select the most definitive.

V. **Origin.** Place an "X" in one of the six boxes.
Original Proceedings. (1) Cases which originate in the United States district courts.
Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441. When the petition for removal is granted, check this box.
Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
Multidistrict Litigation. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407. When this box is checked, do not check (5) above.

VI. **Cause of Action.** Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service; **OR "AP Docket."**

VII. **Requested in Complaint.** Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

VIII. **Related Cases.** This section of the JS 44 is used to reference related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.