IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO

ALLISON WILMOT, individually and on behalf of all others similarly situated, Plaintiff, v. **SM ENERGY COMPANY,** Defendant.	**Case No.** 1:26-cv-03596 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Allison Wilmot, ("Plaintiff"), individually and on behalf of all others similarly situated (the "Class" or "Class Members," as defined below), by and through her undersigned counsel, files this Class Action Complaint against SM Energy Company ("SM Energy" or "Defendant") and alleges the following based on personal knowledge of facts, upon information and belief, and based on the investigation of her counsel as to all other matters.

I. NATURE OF THE ACTION

1. Plaintiff brings this class action lawsuit against Defendant for its negligent failure to protect and safeguard Plaintiff's and Class Members' highly sensitive personally identifiable information[1] ("PII" or "Private Information"), culminating in a massive and preventable data breach (the "Data Breach" or "Breach"). As a result of Defendant's failure to implement reasonable and necessary data security practices, cybercriminals easily infiltrated Defendant's

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual.

inadequately protected computer systems and stole the Private Information of Plaintiff and Class Members.

2. Defendant is an oil and natural gas exploration and production company with active operations in Colorado, Texas, and Utah.[2]

3. As part of its business practices and to provide services, Defendant collects, stores, and maintains customers' and employees' PII, including Plaintiff's and Class Members'. Plaintiff and Class Members are current and former customers and employees of Defendant.

4. On or about May 15, 2026, Defendant discovered that unauthorized cybercriminals gained access to Defendant's inadequately protected computer system and extracted Plaintiff's and the Class Member's Private Information stored thereon.[3] Upon information and belief, Defendant has not disclosed publicly what threat actor was involved.

5. Defendant reported to the Texas Attorney General that at least 3,851 Texas residents were affected by the Breach.[4]

6. The Defendant disclosed in its report to the California Attorney General that at least the following pieces of sensitive personal information were included in the Breach: name, postal address, email, phone number, and Social Security number/Taxpayer Identification number.[5]

7. While the Breach was discovered on or about May 15, 2026, SM Energy delayed noticing affected individuals until around July 30, 2026, when SM Energy began mailing notice

[2] https://www.sm-energy.com/about-us (last visited August 7, 2026).

[3] https://www.mass.gov/doc/2026-1258-sm-energy-company/download (last visited August 7, 2026).

[4] https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage (last visited August 7, 2026).

[5] https://oag.ca.gov/system/files/EXP_Q2216_SME_DBM-5880_L01_SAS_1.pdf (last visited August 7, 2026).

letters ("Notice Letter") to affected individuals.[6] Defendant's Notice Letter states that at least names, postal address, email address, phone number, and Social Security number/Taxpayer Identification number were involved in the Data Breach.[7] Defendant's delay in alerting impacted individuals of the Breach prevented Plaintiff and Class Members from taking earlier actions to protect themselves against fraud and misuse of their information.

8. Plaintiff and Class Members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would safeguard their Private Information from unauthorized disclosure and would implement sufficient cybersecurity safeguards to protect such information.

9. Businesses that store and maintain customers' and employees' Private Information, like Defendant, owe the individuals to whom the information relates a duty to adopt reasonable measures to protect it from unauthorized disclosures and unauthorized third parties. This duty arises under contract, statutory and common law, industry standards, representations made to Plaintiff and Class Members, and because it is foreseeable that the exposure of Private Information to unauthorized persons, and especially hackers, will harm the affected individuals, including to the invasion of their private information and financial matters.

10. In providing their Private Information to Defendant, Plaintiff and the Class Members reasonably expected this sophisticated business entity to keep their Private Information confidential and secured from unauthorized disclosures, to use this information for business purposes only, and to disclose it only as authorized. Defendant failed to do so, resulting in the unauthorized disclosure of Plaintiff's and Class Members' Private Information in the Breach.

[6] Exhibit 1 – Notice of Data Breach
[7] *Id.*

11. Defendant failed to adequately protect Plaintiff's and Class Members' Private Information and failed to ensure that it would maintain adequate safeguards to protect its customers' and employees' Private Information.

12. Upon information and belief, Plaintiff's and Class Members' Private Information is in the hands of cybercriminals who will continue to use the stolen Private Information for nefarious purposes for the rest of their lives.

13. Due to Defendant's negligent failure to secure and protect Plaintiff's and Class Members' Private Information, cybercriminals have stolen and obtained everything they need to commit identity theft and wreak havoc on the financial and personal lives of thousands of individuals.

14. Now, and for the rest of their lives, Plaintiff and the Class Members will have to deal with the danger of identity thieves possessing and misusing their Private Information. Even those Class Members who have yet to experience identity theft will have to spend time responding to the Data Breach and are at an immediate and heightened risk of all manners of identity theft as a direct and proximate result of the Data Breach.

15. Plaintiff and Class Members have incurred and will continue to incur damages in the form of, among other things, identity theft, attempted identity theft, lost time and expenses mitigating harms, increased risk of harm, damaged credit, diminution of the value of their Private Information, loss of privacy, and additional damages as described below.

16. Plaintiff brings this action individually and on behalf of the Class, seeking compensatory damages, punitive damages, nominal damages, restitution, injunctive and declaratory relief, reasonable attorneys' fees and costs, and all other remedies this Court deems just and proper.

II. THE PARTIES

17. Plaintiff **Allison Wilmot** is an individual domiciled in Broomfield, Colorado, who resides on property where Defendant has an oilwell it services. Plaintiff Wilmot received a Notice Letter from the Defendant dated July 30, 2026, informing her that her sensitive personal information, including name, address, email, phone number, and Social Security number/Taxpayer identification number, were involved in the Breach. *See* **Exhibit 1.**

18. Defendant **SM Energy Company** is a Delaware corporation with its headquarters and principal place of business located at 1700 N Lincoln Street, Suite 3200, Denver, Colorado 80203. Defendant's service agent is Corporation Service Company, located at 1900 W Littleton Boulevard, Littleton, Colorado 80120.

III. JURISDICTION AND VENUE

19. This Court has subject-matter jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d) because (1) the matter in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, (2) the action is a class action, (3) numerous Class Members are citizens of a different state that is diverse from Defendant,[8] and (4) there are more than 100 Class Members.

20. This Court has personal jurisdiction over Defendant because its principal place of business is in Colorado, and the acts and omissions giving rise to Plaintiff's claims occurred in this State.

[8] There are at least 3,851 Texas residents that are Class Members. https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage (last visited August 7, 2026).

21. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(1) because Defendant's principal place of business is in this District, and a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

IV. FACTUAL ALLEGATIONS

A. Defendant Collected Plaintiff's and Class Members' Private Information.

22. Defendant is an oil and natural gas exploration and production company with active operations in Colorado, Texas, and Utah.[9]

23. As part of its business practices and to provide services, Defendant collects, stores, and maintains customers' and employees' PII, including Plaintiff's and Class Members'. Plaintiff and Class Members are current and former customers and employees of Defendant.

24. Defendant obtains, collects, uses, and derives a benefit from the Private Information of Plaintiff and Class Members. Defendant uses the Private Information it collects to provide employment and services, making a profit therefrom. Defendant would not be able to obtain revenue if not for the acceptance and use of Plaintiff's and the Class's Private Information.

25. Defendant would be unable to engage in its regular business activities without collecting and aggregating Private Information it knows and understands to be sensitive and confidential.

26. Upon information and belief, Defendant made promises and representations to its customers and employees, and indirectly to Plaintiff and Class Members, that the Private Information collected from them would be kept safe and confidential, and that the privacy of that information would be maintained.

[9] https://www.sm-energy.com/about-us (last visited August 7, 2026).

27. Class Members who are current and former customers of Defendant paid Defendant, directly or indirectly, for services. Defendant promised data security to its customers as part of these financial services and part of this payment should have been specifically allocated to data security.

28. Class Members who are current and former employees of Defendant allowed Defendant to make a profit from their services and labor. Defendant promised data security to its employees as part of their employment and part of the revenue earned through the labor of its employees should have been specifically allocated to data security.

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

30. Plaintiff and the Class Members reasonably relied on Defendant's promises to keep their Private Information secure, as Defendant intended

31. Plaintiff and Class Members provided their Private Information, directly or indirectly, to Defendant with the reasonable expectation and on the mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

32. Upon information and belief, Defendant failed to adopt reasonable and appropriate data security practices and procedures including administrative, physical security, and technical controls to safeguard Plaintiff's and the Class's Private Information.

33. As a result of collecting and storing the Private Information of Plaintiff and Class Members for its own financial benefit, Defendant had a continuous duty to adopt and employ

reasonable measures to protect Plaintiff's and the Class Members' Private Information from disclosure to third parties, and to audit, monitor, and verify the integrity and cybersecurity of its systems storing Private Information.

B. Defendant's Data Breach.

34. On or about May 15, 2026, Defendant discovered that unauthorized cybercriminals gained access to Defendant's inadequately protected computer system and extracted Plaintiff's and the Class Member's Private Information stored thereon.[10] Upon information and belief, Defendant has not disclosed publicly what threat actor was involved.

35. The Defendant disclosed in its report to the California Attorney General that at least the following pieces of sensitive personal information were included in the Breach: name, postal address, email, phone number, and Social Security number/Taxpayer Identification number.[11]

36. While the Breach was discovered on or about May 15, 2026, SM Energy delayed noticing affected individuals until around July 30, 2026, when SM Energy began mailing Notice Letters to affected individuals.[12] Defendant's delay in alerting impacted individuals of the Breach prevented Plaintiff and Class Members from taking earlier actions to protect themselves against fraud and misuse of their information.

37. Defendant's delayed notice of the Breach leaves impacted individuals with no information regarding critical facts about the Data Breach, such as details of the root cause of the Breach, the vulnerabilities exploited, when the Breach occurred, and the remedial measures taken by Defendant, if any.

---

[10] https://www.mass.gov/doc/2026-1258-sm-energy-company/download (last visited August 7, 2026).

[11] https://oag.ca.gov/system/files/EXP_Q2216_SME_DBM-5880_L01_SAS_1.pdf (last visited August 7, 2026).

[12] Exhibit 1

38. Defendant failed to take the necessary precautions required to safeguard and protect Plaintiff's and Class Members' Private Information from unauthorized access and exploitation.

39. Defendant failed to timely notify Plaintiff and Class Members of the Data Breach.

40. By collecting, storing, and maintaining the Private Information of Plaintiff and Class Members, Defendant owed a duty to Plaintiff and Class Members to protect and safeguard their Private Information from unauthorized disclosures.

41. Plaintiff's and Class Members' Private Information was targeted, accessed, and stolen by cybercriminals in the Data Breach. Defendant's deficient security for customer and employee data caused and allowed criminals to target and take files containing Plaintiff's and Class Members' inadequately protected, unencrypted Private Information in Defendant's possession through the Data Breach.

42. Because Defendant had a duty to protect Plaintiff's and Class Members' Private Information, Defendant should have known through readily available and accessible information about potential threats for the unauthorized exfiltration and misuse of such information. Thus, Defendant had a duty to ensure that customers' and employees' Private Information, stored within its networks and systems, was secured and protected from unauthorized disclosures to third parties.

43. Defendant could and should have prevented this Data Breach by ensuring the files and servers containing Plaintiff's and Class Members' Private Information were properly secured and encrypted but failed to do so.

44. Defendant could have prevented the Data Breach by properly securing and encrypting the files and servers containing the Private Information of Plaintiff and Class Members. This Data Breach could have been prevented through industry standard network segmentation and

encryption of confidential information. Further, the Data Breach could have likely been prevented had Defendant utilized appropriate malware prevention and detection technologies

45. Plaintiff further believes that her Private Information and that of Class Members, was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

46. All in all, Defendant failed to take the necessary precautions required to safeguard and protect Plaintiff's and Class Members' Private Information from unauthorized access and exploitation.

47. Defendant's actions represent a flagrant disregard of the rights of Plaintiff and the Class, both as to privacy and property.

48. As such, Plaintiff and the Class have suffered harm and continue to be at an imminent and impending risk of identity theft and fraud.

C. Cyber Criminals Will Use Plaintiff's and Class Members' Private Information to Defraud them.

49. Private Information is of great value to hackers and cybercriminals, and the data stolen in the Data Breach can and will be used in a variety of ways by criminals to exploit Plaintiff and Class Members and to profit off their misfortune.

50. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[13]

51. For example, with the Private Information stolen in the Data Breach, including Social Security numbers, identity thieves can open financial accounts, apply for credit, obtain

[13] *Facts + Statistics: Identity Theft and Cybercrime*, INSURANCE INFO. INST., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (last visited Feb. 19, 2026).

medical services, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft.[14]

52. These criminal activities have and will result in devastating financial and personal losses to Plaintiff and Class Members.

53. When cybercriminals manage to steal personally sensitive data like Social Security numbers—as they did here—there is no limit to the amount of fraud to which Plaintiff and Class Members are exposed.

54. Social Security numbers are particularly sensitive pieces of personal information. As the Consumer Federation of America explains:

> **Social Security number.** *This is the most dangerous type of personal information in the hands of identity thieves* because it can open the gate to serious fraud, from obtaining credit in your name to impersonating you to get medical services, government benefits, your tax refunds, employment – even using your identity in bankruptcy and other legal matters. It's hard to change your Social Security number and it's not a good idea because it is connected to your life in so many ways.[15]
>
> (Emphasis added).

[14] *See, e.g.*, Nikkita Walker, What Can You Do With Your Social Security Number, Credit.com (Oct. 19, 2023), https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/.

[15] Dark Web Monitoring: What You Should Know, Consumer Federation of America (Mar. 19, 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

55. PII is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it for years.[16]

56. The Data Breach at issue here was targeted and financially motivated, as the only reason cybercriminals go through the trouble of hacking entities like Defendant is to steal the highly sensitive information they maintain, which can be exploited and sold for use in the kinds of criminal activity described herein.

57. A Social Security number, date of birth, and full name can sell for $60 to $80 on the digital black market.[17]

58. Identity theft experts advise victims of data breaches: "[I]f there is reason to believe that your personal information has been stolen, you should assume that it can end up for sale on the dark web."[18]

59. These risks are both certainly impending and substantial. As the Federal Trade Commission ("FTC") has reported, if hackers get access to PII, **they will use it**.[19]

60. Hackers may not use the information right away, but this does not mean it will not be used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

---

[16] *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (July 5, 2007), https://www.gao.gov/products/gao-07-737.

[17] Michael Kan, Here's How Much Your Identity Goes for on the Dark Web, PGMag (Nov. 15, 2017), https://www.pcmag.com/news/heres-how-much-your-identity-goes-for-on-the-dark-web.

[18] *Dark Web Monitoring: What You Should Know*, Consumer Federation of America (Mar. 19, 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

[19] Ari Lazarus, *How fast will identity thieves use stolen info?*, Military Consumer (May 24, 2017), https://www.militaryconsumer.gov/blog/how-fast-will-identity-thieves-use-stolen-info.

> [I]n 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.[20]

61. For instance, with a stolen Social Security number, which was information in possession by the Defendant and included in the Breach, criminals can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.[21]

62. Identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit as well as protecting themselves in the future.[22]

63. The unfortunate truth is the full scope of the harm has yet to be realized. There may be a time lag between when harm occurs and when it is discovered, and also between when Private Information is stolen and when it is used.

64. Plaintiff and Class Members will need to pay for their own identity theft protection and credit monitoring for the rest of their lives due to Defendant's negligence.

65. Furthermore, identity monitoring services only alert someone to the fact that they have already been the victim of identity theft—it does not prevent identity theft.[23]

---

[20] *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (July 5, 2007), https://www.gao.gov/products/gao-07-737 (emphasis added).

[21] *See* Nikkita Walker, *What Can Someone Do with Your Social Security Number?*, Credit.com (Oct. 19, 2023), https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/.

[22] *Guide for Assisting Identity Theft Victims*, Federal Trade Commission (Sept. 2013), https://www.global-screeningsolutions.com/Guide-for-Assisting-ID-Theft-Victims.pdf.

[23] *See* Kayleigh Kulp, *Credit monitoring services may not be worth the cost*, CNBC (Nov. 30, 2017, 9:00 AM), https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-be-worth-the-cost.html.

66. Nor can an identity monitoring service remove personal information from the dark web.[24]

67. "The people who trade in stolen personal information [on the dark web] won't cooperate with an identity theft service or anyone else, so it's impossible to get the information removed, stop its sale, or prevent someone who buys it from using it."[25]

68. As a direct and proximate result of the Data Breach, Plaintiff and the Class have been damaged and placed at an imminent and continuing increased risk of harm from fraud and identity theft. Plaintiff and the Class must now take the time and effort to mitigate the actual and potential impact of the Data Breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and medical records for unauthorized activity for years to come.

69. Even more serious is the identity restoration that Plaintiff and other Class Members must go through, which can require spending countless hours filing police reports, filling out IRS forms, completing Federal Trade Commission checklists and Department of Motor Vehicle driver's license replacement applications, and calling financial institutions to cancel fraudulent credit applications, to name just a few of the steps Plaintiff and the Class must take.

70. Plaintiff and the Class have or will experience the following concrete and particularized harms for which they are entitled to compensation, including:

a. Actual identity theft;

[24] *Dark Web Monitoring: What You Should Know*, Consumer Federation of America (Mar. 19, 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

[25] *Id.*

b. Trespass, damage to, and theft of their personal property, including their Private Information;

c. Improper disclosure and theft of their Private Information;

d. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Private Information being placed in the hands of criminals;

e. Loss of privacy suffered as a result of the Data Breach, including the harm of knowing cybercriminals have their Private Information;

f. Ascertainable losses in the form of time taken to respond to identity theft, including lost opportunities and lost wages from uncompensated time off from work;

g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the Data Breach;

h. Ascertainable losses in the form of diminution of the value of Plaintiff's and Class Members' Private Information, for which there is a well-established and quantifiable national and international market;

i. The loss of use of and access to their credit, accounts, and/or funds;

j. Damage to their credit due to fraudulent use of their Private Information; and/or

k. Increased cost of borrowing, insurance, deposits, and the inability to secure more favorable interest rates because of a reduced credit score.

71. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which remains in the possession of Defendant, is protected from further breaches through the implementation of industry standard security measures and safeguards.

Defendant has shown itself wholly incapable of protecting Plaintiff's and Class Members' Private Information.

72. Plaintiff and Class Members also have an interest in ensuring that their Private Information is removed from all Defendant's servers, systems, and files.

73. Plaintiff and Class Members are desperately trying to mitigate the damages Defendant caused them.

74. Given the kind of Private Information Defendant made accessible to hackers, however, Plaintiff and the Class are certain to incur additional damages. Because identity thieves have their Private Information, Plaintiff and Class Members will need to have identity theft monitoring protection for the rest of their lives. Some may even need to go through the long and arduous process of getting a new Social Security number, with all the loss of credit and employment difficulties that come with a new number.[26]

75. None of this should have happened because the Data Breach was entirely preventable.

D. Defendant was Aware—or Should Have Been Aware—of the Risk of Cyberattacks.

76. Data security breaches have dominated the headlines for the last two decades. And it doesn't take an IT industry expert to know it. The general public can tell you the names of

[26] *What happens if I change my Social Security number?*, Lexington Law (Aug. 10, 2022), https://www.lexingtonlaw.com/blog/credit-101/will-a-new-social-security-number-affect-your-credit.html.

some of the biggest cybersecurity breaches: Target,[27] Yahoo,[28] Marriott International,[29] Chipotle, Chili's, Arby's,[30] and others.[31]

77. The number of data breach victims has surpassed 1 billion for the first half of 2024, according to the Identity Theft Resource Center.[32]

78. Defendant should certainly have been aware, and indeed was aware, that it was at risk of a data breach that could expose the PII that it collected and maintained.

79. Defendant was clearly aware of the risks it was taking and the harm that could result from inadequate data security but threw caution to the wind.

80. SM Energy (1) had deficient security measures to protect the Private Information it stored for its current and former customers and employees; (2) was aware or should have been aware of the risk of harm to its customers and employees in the event of a data breach; (3) knew or should have known of the foreseeable harms caused by cyberattacks; and (4) negligently failed to safeguard Plaintiff's and Class Members' Private Information.

---

[27] Michael Kassner, *Anatomy of the Target Data Breach: Missed Opportunities and Lessons Learned*, ZDNET (Feb. 2, 2015), https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/.

[28] Martyn Williams, *Inside the Russian Hack of Yahoo: How They Did It*, CSOONLINE.COM (Oct. 4, 2017), https://www.csoonline.com/article/3180762/inside-the-russian-hack-of-yahoo-how-they-did-it.html.

[29] Patrick Nohe, *The Marriot Data Breach: Full Autopsy*, THE SSL STORE: HASHEDOUT (Mar. 22, 2019), https://www.thesslstore.com/blog/autopsying-the-marriott-data-breach-this-is-why-insurance-matters/ (last visited Feb. 6, 2026).

[30] Alfred Ng, *FBI Nabs Alleged Hackers in Theft of 15M Credit Cards from Chipotle, Others*, CNET (Aug. 1, 2018, 12:58 PM), https://www.cnet.com/news/fbi-nabs-alleged-hackers-in-theft-of-15m-credit-cards-from-chipotle-others/?ftag=CMG-01-10aaa1b.

[31] *See, e.g.*, Michael Hill and Dan Swinhoe, *The 15 Biggest Data Breaches of the 21st Century*, CSO ONLINE (Nov. 8, 2022), https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.

[32] https://www.usatoday.com/story/money/2024/07/18/data-breach-what-to-do/74441060007/.

81. Despite its assurances to customers and employees regarding safeguarding PII, Defendant negligently failed to implement adequate security measures to safeguard the Private Information of Plaintiff and Class Members.

E. Defendant Failed to Comply with Federal Trade Commission Guidelines and Industry Standards for Cybersecurity.

82. Data breaches are preventable.[33] "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[34] "Organizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised[.]"[35]

83. Most reported data breaches "are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures. . . . Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[36]

84. Here, many failures laid the groundwork for the Data Breach.

85. The FTC has published guidelines that establish reasonable data security practices for businesses.[37]

---

[33] Lucy L. Thomson, *Despite the Alarming Trends, Data Breaches Are Preventable*, Data Breach and Encryption Handbook (Lucy Thompson, ed., 2012), available at https://lawcat.berkeley.edu/record/394088.

[34] *Id.* at 17.

[35] *Id.* at 28.

[36] *Id.*

[37] *Protecting Personal Information: A Guide for Business*, FTC (Oct. 2016), available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

86. The FTC guidelines emphasize the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.[38]

87. The FTC guidelines establish that businesses should protect the confidential information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems.[39]

88. The FTC guidelines also recommend that businesses utilize an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating hacking attempts; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[40]

89. According to information and belief, Defendant failed to follow reasonable and necessary industry standards to prevent the Breach, including the FTC's guidelines.

90. Upon information and belief, Defendant also failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework, NIST Special Publications 800-53, 53A, or 800-171; the Federal Risk and Authorization Management Program (FEDRAMP); or the Center for Internet Security's Critical Security Controls (CIS CSC), which are well respected authorities in cybersecurity readiness.

91. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[41]

---

[38] *Id.*
[39] *Id.*
[40] *Id.*
[41] *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.

92. To prevent and detect the attack here, Defendant could and should have taken, as recommended by the Federal Bureau of Investigation, the following measures:

- Implemented 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.
- Enabled 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.
- Scanned all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configured firewalls to block access to known malicious IP addresses.
- Patched operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Managed 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.

- Configured 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.
- Disabled 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.
- Implemented 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.
- Considered disabling Remote Desktop protocol (RDP) if it is not being used.
- Used application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Executed operating system environments or specific programs in a virtualized environment.
- Categorized data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[42]

93. According to information and belief, Defendant failed to do any of the above.

94. To prevent and detect ransomware attacks, Defendant could and should have recommended its employees, as recommended by the United States Cybersecurity & Infrastructure Security Agency, take the following measures:

[42] *Id.* at 3–4.

- **Updated and patched 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.
- **Used caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net).
- **Opened 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.
- **Kept your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it.
- **Verified 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.

- **Used and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic.[43]

95. In addition, to prevent and detect the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

- **Harden internet-facing assets**
  - Apply latest security updates
  - Use threat and vulnerability management
  - Perform regular audits
- **Thoroughly investigate and remediate alerts.**
  - Prioritize and treat commodity malware infections as potential full compromise of the system
- **Include IT professionals in security discussions.**
  - Ensure collaboration among security operations, security administrators, and information technology administrators to configure servers and other endpoints securely

[43] *See Protecting Against Ransomware*, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (revised Sept. 2, 2021), https://www.cisa.gov/news-events/news/protecting-against-ransomware (internal citations omitted).

- **Build and maintain credential hygiene**
    - Use multifactor authentication or network level authentication and enforce strong, randomized, just-in-time local administrator 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**
    - Utilize 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[44]

96. Given that Defendant was storing the Private Information of thousands of individuals, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks. However, Defendant failed to do so because an unknown third-party was able to gain access to Defendant's inadequately secured network and systems and exfiltrate the sensitive Private Information of Plaintiff and Class Members.

[44] *See Human-operated ransomware attacks: A preventable disaster*, MICROSOFT THREAT Intelligence (Mar 5, 2020), https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/.

97. Specifically, among other failures, Defendant had far too much confidential unencrypted information held on its systems. Such Private Information should have been segregated into an encrypted system.[45]

98. Moreover, it is well-established industry standard practice for a business to dispose of confidential Private Information once it is no longer needed.[46]

99. The FTC has repeatedly emphasized the importance of disposing of unnecessary Private Information: "Keep sensitive data in your system only as long as you have a business reason to have it. Once that business need is over, properly dispose of it. If it's not on your system, it can't be stolen by hackers."[47] Rather than following this basic standard of care, Defendant kept thousands of customers' and employees' unencrypted Private Information on its inadequately secured systems indefinitely.

100. In sum, the Data Breach could have been easily prevented through standard practices like the use of industry standard network segmentation and encryption of all Private Information—which Defendant negligently failed to do.

101. Further, the scope of the Data Breach could have been dramatically reduced had Defendant utilized proper record retention and destruction practices—but Defendant negligently did no such thing.

---

[45] *See* Adnan Raja, *How to Safeguard Your Business Data With Encryption*, DATAINSIDER (Aug. 14, 2018), https://digitalguardian.com/blog/how-safeguard-your-business-data-encryption.

[46] *See Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (Oct. 2016), https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business.

[47] *Id.* at 6.

F. Common Injuries and Damages.

102. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to the Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) nominal damages; and (viii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains 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 Private Information.

G. Loss of Time to Mitigate the Risks of Fraud and Identity Theft.

103. As a result of the recognized risk of identity theft, when a data breach occurs, and an individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm—yet the asset of time has been lost.

104. Due to the actual and imminent risk of identity theft, Plaintiff and Class Members must monitor their financial accounts for many years to mitigate that harm. Identity theft protection

and credit monitoring services are reasonable and necessary for Plaintiff and Class Members to protect themselves against fraud and identity theft. Plaintiff and Class Members will have to pay for these services for the rest of their lives now that their Private Information has been accessed and exposed in Defendant's Breach.

105. Plaintiff and Class Members have spent time, and will spend additional time in the future, on a variety of prudent actions, such as placing freezes and alerts with credit reporting agencies, contacting financial institutions, closing or modifying financial accounts, changing passwords, reviewing and monitoring credit reports and accounts for unauthorized activity, and filing police reports, which may take years to discover.

106. These efforts are consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.

107. Once Private Information is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff and Class Members will need to maintain these heightened measures for years, and possibly their entire lives, as a result of Defendant's conduct that caused the Data Breach.

H. Future Cost of Credit and Identity Theft Monitoring is Reasonable and Necessary.

108. To date, Defendant has done nothing to provide Plaintiff and Class Members with relief for the damages they have suffered due to the Data Breach.

109. Given the type of targeted attack in this case and sophisticated criminal activity, the type of information involved, and the *modus operandi* of cybercriminals, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes— e.g., opening bank accounts in the victims' names to make purchases or to launder money; filing false tax returns; taking out loans or insurance; or filing false unemployment claims.

110. By accessing and obtaining the PII in the Breach, hackers have everything they need to commit fraud and identity theft.

111. Such fraud may go undetected until debt collection calls commence months, or even years later. An individual may not know that her or her information was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

112. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel their cards and request a replacement.[48]

113. The information disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

114. Consequently, Plaintiff and Class Members are at a present and ongoing risk of fraud and identity theft for many years into the future.

[48] Jesse Damiani, Your Social Security Number Costs $4 On The Dark Web, New Report Finds, FORBES (Mar. 25, 2020), https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-securitynumber-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1 (last visited Feb. 11, 2025).

115. The retail cost of credit monitoring and identity theft monitoring can cost $200 or more a year per Class Member. This is a reasonable and necessary cost to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach. This is a future cost for a minimum of five years that Plaintiff and Class Members would not need to bear but for Defendant's failure to safeguard their Private Information.

I. Plaintiff's Individual Experience

Plaintiff Allison Wilmot

116. Plaintiff Wilmot resides on property where Defendant has an oil well it services and was required to provide her Private Information, including Social Security number, to Defendant as part of Defendant's business practices.

117. Plaintiff Wilmot received a notice letter from the Defendant postmarked July 30, 2026, informing her that at least her name, postal address, email, phone number, and Social Security number/Taxpayer Identification number were included in the Breach.[49]

118. Plaintiff entrusted her Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would keep her Private Information secure from unauthorized access.

119. By soliciting and accepting Plaintiff 's Private Information, Defendant agreed to safeguard and protect it from unauthorized access and delete it after a reasonable time.

120. Plaintiff Wilmot would not have provided her Private Information to Defendant had she known it would be kept using inadequate data security and vulnerable to a cyberattack.

121. Upon information and belief, Defendant was in possession of Plaintiff 's Private Information before, during, and after the Data Breach.

[49] Exhibit 1

122. As a result, Plaintiff Wilmot was injured by Defendant's Data Breach.

123. In response to the Data Breach, upon information and belief, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to researching the Data Breach, reviewing and monitoring her accounts for fraudulent activity, and reviewing her credit reports. Upon information and belief, Plaintiff estimates she has already spent hours responding to the Data Breach.

124. Plaintiff will be forced to spend additional time reviewing her credit reports and monitoring her accounts for the rest of her life. This is time spent which has been lost forever and cannot be recaptured.

125. Plaintiff places significant value in the security of her Private Information and does not readily disclose it. Plaintiff entrusted Defendant with her Private Information with the understanding that Defendant would keep her information secure and would employ reasonable and adequate data security measures to ensure that her Private Information would not be compromised.

126. Because of the Data Breach, there is no doubt Plaintiff 's highly confidential Private Information is in the hands of cybercriminals. Reason being, the *modus operandi* of cybercriminals is to steal data they can exploit by selling on the dark web. As such, Plaintiff and the Class are at an imminent risk of identity theft and fraud.

127. Plaintiff Wilmot suffered actual injury from the exposure and theft of her Private Information—which violates her rights to privacy.

128. Plaintiff Wilmot suffered actual injury in the form of damages to and diminution in the value of her Private Information. After all, PII is a form of intangible property—property that Defendant was required to adequately protect and safeguard against unauthorized disclosure.

129. Due to Defendant's Breach, Plaintiff will be forced to spend money to cover the cost of future credit monitoring and identity-theft monitoring, given the type of data stolen in the Breach and the fact that, upon information and belief, her information has already been published on the dark web. The need for future monitoring is reasonable and necessary and is a consequence of Defendant's breach of duty to maintain Plaintiff 's highly sensitive Private Information, including her Social Security number, secure and protected against unauthorized disclosure.

130. Plaintiff 's highly sensitive Private Information accessed in the Breach provides hackers with a clear ability to commit fraud.

131. Knowing that thieves intentionally targeted and accessed her Private Information, has caused Plaintiff great anxiety beyond mere worry.

132. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by Defendant's delay in notifying her of the fact that her Private Information was accessed and/or acquired by criminals as a result of the Data Breach.

133. Plaintiff has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source.

134. As a direct and traceable result of the Data Breach, Plaintiff suffered actual injury and damages after her Private Information was compromised and stolen in the Data Breach, including, but not limited to: (i) lost time and money related to monitoring her accounts and credit reports for fraudulent activity; (ii) loss of privacy due to her Private Information being accessed and stolen by cybercriminals; (iii) loss of the benefit of her bargain because Defendant did not adequately protect her Private Information; (iv) emotional distress because identity thieves now possess her Private Information; (v) imminent and impending injury arising from the increased risk of fraud and identity theft now that her Private Information has been stolen and published on

the dark web; (vi) diminution in the value of her Private Information, a form of intangible property that Defendant obtained from Plaintiff ; and (vii) other economic and non-economic harm.

135. Plaintiff has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for ***years*** to come. This risk is certainly real and impending, and is not speculative, given the highly sensitive nature of the Private Information stolen in the Data Breach.

136. Plaintiff has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains in the possession of Defendant, is protected, and safeguarded from future data breaches. Absent Court intervention, Plaintiff 's Private Information will be wholly unprotected and at-risk of future data breaches.

V. CLASS ACTION ALLEGATIONS

137. Plaintiff incorporates by reference all preceding factual paragraphs as if fully restated here.

138. Plaintiff brings this action against Defendant individually and on behalf of all others similarly situated under Federal Rule of Civil Procedure 23. Plaintiff asserts all claims on behalf of the class (the "Class") defined as follows:

> **All persons whose PII was accessed and/or compromised as a result of the Data Breach, including all persons that were sent a Notice Letter.**

139. Excluded from the Class is Defendant, any entity in which Defendant has a controlling interest, and Defendant's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class is any judge, justice, or judicial officer presiding over this matter and members of their immediate families and their judicial staff members.

140. Plaintiff reserves the right to amend or modify the above Class definition or to propose subclasses in subsequent pleadings and motions for class certification.

141. Plaintiff anticipates the issuance of notice setting forth the subject and nature of the instant action to the proposed Class. Upon information and belief, Defendant's own business records or electronic media can be utilized for the notice process.

142. The proposed Class meets the requirements of FRCP 23.

143. **Numerosity.** Class Members are so numerous that joinder of all members is impracticable. The Defendant reported that at least 3,851 individuals were impacted by the Breach, but the total number of affected individuals is not publicly available.[50] Upon information and belief, the Class consists of thousands of individuals affected by the Data Breach. Each Class Member is apparently identifiable within Defendant's records.

144. **Typicality.** Plaintiff's claims are typical of the claims of the Class because Plaintiff's Private Information, like that of every other Class Member, was compromised in the Data Breach. Plaintiff and all members of the Class were injured by the same wrongful acts, practices, and omissions committed by Defendant, as described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that gives rise to the claims of all Class Members.

145. **Adequacy of Representation.** Plaintiff is an adequate representative of the Class because Plaintiff's interests do not conflict with the interests of the Class. Plaintiff has retained counsel competent and highly experienced in data breach class action litigation, and Plaintiff and

[50] https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage (last visited August 7, 2026).

Plaintiff's counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and her counsel.

146. **Superiority**. A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiff and the Class. The injury suffered by each individual Class Member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for individual members of the Class to effectively redress Defendant's wrongdoing. Even if Class Members could afford such individual litigation, the court system could not. Individualized litigation presents potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

147. **Commonality and Predominance.** Defendant engaged in a common course of conduct toward Plaintiff and Class Members, in that Plaintiff's and Class Members' Private Information was stored on the same network and unlawfully accessed in the same way. There are many questions of law and fact common to the claims of Plaintiff and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

a. Whether Defendant engaged in the wrongful conduct alleged herein;

b. Whether Defendant owed a duty to Plaintiff and Class Members to adequately protect their Private Information;

c. Whether Defendant breached its duty to Plaintiff and Class Members to adequately protect their Private Information;

d. 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;

e. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

f. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

g. Whether Defendant knew or should have known that its computer and network security systems, or the computer and network security systems of its vendors, were vulnerable to cyberattacks;

h. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the Data Breach;

i. Whether Defendant was negligent in permitting unencrypted Private Information belonging to thousands of individuals to be stored within their network;

j. Whether Defendant was negligent in failing to adhere to reasonable data retention policies;

k. Whether Defendant breached implied contractual duties to Plaintiff and the Class to use reasonable care in protecting their Private Information;

l. Whether Defendant was unjustly enriched by unlawfully retaining a benefit conferred upon it by Plaintiff and Class Members;

m. Whether Defendant should have discovered the Data Breach sooner;

n. Whether Defendant failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiff and the Class;

o. Whether Defendant continues to breach duties owed to Plaintiff and the Class;

p. Whether Plaintiff and the Class suffered injuries as a proximate result of Defendant's negligent actions or failures to act;

q. Whether Defendant was negligent in selecting, supervising, and/or monitoring vendors;

r. Whether Plaintiff and the Class are entitled to recover damages, equitable relief, and other relief; and

s. Whether Defendant's actions alleged herein constitute gross negligence, and whether Plaintiff and Class Members are entitled to punitive damages.

148. Common sources of evidence may also be used to demonstrate Defendant's unlawful conduct on a class-wide basis, including, but not limited to, documents and testimony about its data and cybersecurity measures (or lack thereof); testing and other methods that can prove Defendant's data and cybersecurity systems have been or remain inadequate; documents and testimony about the source, cause, and extent of the Data Breach; and documents and testimony about any remedial efforts undertaken as a result of the Data Breach

149. 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 it 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 are representatives 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.

150. 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 demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

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

152. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant 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 and corresponding declaratory 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.

153. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses.

VI. CAUSES OF ACTION

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

154. Plaintiff re-alleges and incorporates by reference paragraphs 1-151 as if fully restated here.

155. Defendant solicited, collected, stored, and maintained the Private Information of Plaintiff and Class Members on inadequately secured computer systems and networks.

156. Upon accepting and storing Plaintiff's and Class Members' Private Information on its computer systems and networks, Defendant undertook and owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their Private Information from unauthorized access and disclosure.

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

158. Defendant's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

159. Defendant had full knowledge of the sensitivity of the Private Information in its possession and the types of harm that Plaintiff and Class Members could and would suffer if the Private Information was wrongfully accessed or disclosed. Plaintiff and Class Members were therefore the foreseeable victims of any inadequate data security practices.

160. Defendant's duty to implement and maintain reasonable data security practices arose as a result of the special relationship that exists between Defendant and consumers, which is recognized by laws and regulations, including, but not limited to, the FTC Act and common law.

161. Defendant was in a superior position to ensure its data security practices were sufficient to protect against the foreseeable risk of harm to Plaintiff and Class Members from a data breach.

162. Defendant knew Plaintiff and Class Members relied on it to protect their Private Information. Plaintiff and Class Members were not in a position to assess the data security practices used by Defendant. Because they had no means to identify Defendant's security deficiencies, Plaintiff and Class Members had no opportunity to safeguard their Private Information from cybercriminals. Defendant exercised control over the Private Information stored on its systems and networks; accordingly, Defendant was best positioned and most capable of preventing the harms caused by the Data Breach.

163. Defendant was aware, or should have been aware, of the fact that cybercriminals routinely target entities storing PII through cyberattacks in an attempt to steal valuable Private Information. In other words, Defendant knew of a foreseeable risk to its data security systems but failed to implement reasonable security measures.

164. Defendant owed Plaintiff and Class Members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiff and the Class when obtaining, storing, using, and managing their Private Information, including taking action to reasonably safeguard or delete such data and providing notification to Plaintiff and Class Members of any breach in a timely manner so that appropriate action could be taken to minimize losses.

165. Defendant's duty extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to such risk, or defeats protections put in place to guard against that risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B.

166. Defendant had a duty to implement and maintain reasonable data security practices pursuant to Section 5 of the FTC Act, 15 U.S.C. § 45(a), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect sensitive and confidential data.

167. 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 formed part of the basis of Defendant's duty in this regard.

168. Defendant solicited, collected, stored, and maintained Plaintiff's and Class Members' Private Information as part of their regular business, which affects commerce.

169. Defendant violated the FTC Act by failing to use reasonable measures to protect Plaintiff's and Class Members' Private Information and by failing to comply with applicable industry standards, as described herein.

170. Defendant breached its duties to Plaintiff and the Class under the FTC Act by failing to implement and maintain fair, reasonable, and adequate data security practices to safeguard Plaintiff's and Class Members' Private Information, and by failing to provide prompt notice of the Data Breach without unreasonable delay.

171. Defendant's multiple failures to comply with applicable laws and regulations constitute negligence *per se*.

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

173. 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, like Defendant, that fail to employ reasonable data security measures and avoid unfair and deceptive practices, causing the same harm as that suffered by Plaintiff and the Class.

174. Defendant breached its duties to Plaintiff and the Class by unreasonably delaying and failing to provide notice of the Data Breach expeditiously and/or as soon as practicable to Plaintiff and the Class.

175. Defendant's violations of the FTC Act constitute negligence *per se*.

176. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have suffered, and continue to suffer, damages arising from the Data Breach, as alleged above.

177. The injury and harm that Plaintiff and Class members suffered (as alleged above) was the direct and proximate result of Defendant's negligence *per se*.

178. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Plaintiff's and Class Members' Private Information.

179. The specific negligent acts and omissions committed by Defendant include, but are not limited to:

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

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

c. Failing to ensure its email systems had plans in place to maintain reasonable data security safeguards;

d. Failing to implement and maintain adequate mitigation policies and procedures;

e. Allowing unauthorized access to Plaintiff's and Class Members' Private Information;

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

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

180. Defendant's willful failure to abide by its duties to Plaintiff and Class Members was wrongful, reckless, and grossly negligent considering the foreseeable risks and known threats.

181. It was foreseeable that Defendant's failure to use reasonable measures to protect Plaintiff's and Class Members' Private Information would result in injury to Plaintiff and Class Members.

182. Furthermore, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the financial industry.

183. As a direct and proximate result of Defendant's negligent conduct, including, but not limited to, its failure to implement and maintain reasonable data security practices and procedures as described above, Plaintiff and the Class have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

184. Through Defendant's acts and omissions described herein, including but not limited to Defendant's failure to protect the Private Information of Plaintiff and Class Members from being stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the Private Information of Plaintiff and Class Members while it was within Defendant's possession and control.

185. Further, through its failure to provide timely and clear notification of the Data Breach to Plaintiff and Class Members, Defendant prevented Plaintiff and Class Members from taking meaningful, proactive steps to secure their Private Information and mitigate the impact of the Data Breach.

186. Plaintiff and Class Members could have taken actions earlier had they been timely notified of the Data Breach. Yet, Defendant delayed in noticing Plaintiff and Class Members of the Breach.

187. Plaintiff and Class Members could have enrolled in credit monitoring, instituted credit freezes, and changed their passwords, among other things, had they been alerted to the Data Breach more quickly.

188. Plaintiff and Class Members suffered harm from Defendant's delay in notifying them of the Data Breach.

189. As a direct and proximate result of Defendant's conduct, including, but not limited to, Defendant's failure to implement and maintain reasonable data security practices and procedures, Plaintiff and Class Members have suffered or will suffer injury and damages, including, but not limited to: (i) the loss of the opportunity to determine for themselves how their Private Information is used; (ii) the publication and theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, fraud,

and/or unauthorized use of their Private Information, including the need for substantial credit monitoring and identity protection services for an extended period of time; (iv) lost time and opportunity costs associated with efforts expended to address and mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest and recover from fraud and identity theft; (v) costs associated with placing freezes on credit reports and password protections; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their Private Information, which remains 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 Private Information in its continued possession; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised Private Information for the rest of their lives. Thus, Plaintiff and the Class are entitled to damages in an amount to be proven at trial.

190. The damages Plaintiff and the Class have suffered and will suffer (as alleged above) were and are the direct and proximate result of Defendant's negligent conduct.

191. Plaintiff and the Class have suffered cognizable injuries and are entitled to actual and punitive damages in an amount to be proven at trial.

SECOND CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)

192. Plaintiff re-alleges and incorporates by reference paragraphs 1-151 as if fully restated here.

193. Defendant solicited, collected, stored, and maintained Plaintiff's and Class Members' Private Information as part of Defendant's regular business practices.

194. Plaintiff and Class Members were required to provide their Private Information to Defendant, directly or indirectly, in order to receive services and/or employment. Plaintiff and Class Members paid money, or money was paid on their behalf, to Defendant in exchange for services.

195. Defendant solicited and accepted possession of Plaintiff's and Class Members' Private Information for the purpose of providing services and/or employment to Plaintiff and Class Members.

196. In delivering, directly or indirectly, their Private Information to Defendant and paying for services or receiving employment, Plaintiff and Class Members intended and understood that Defendant would adequately safeguard their Private Information.

197. Plaintiff and Class Members reasonably expected that the Private Information they entrusted to Defendant, in order to receive services or as a condition of their employment, would remain confidential and would not be shared or disclosed to criminal third parties.

198. Plaintiff and Defendant had a mutual understanding that Defendant would implement and maintain adequate and reasonable data security practices and procedures to protect Plaintiff's and Class Members' sensitive Private Information. Plaintiff and Defendant also shared an expectation and understanding that Defendant would not share or disclose, whether intentionally or unintentionally, the sensitive Private Information in its possession and control.

199. Based on Defendant's representations, legal obligations, and acceptance of Plaintiff's and Class Members' Private Information, Defendant had a duty to safeguard the Private Information in its possession through the use of reasonable data security practices.

200. When Plaintiff and Class Members paid money and provided their Private Information to Defendant, either directly or indirectly, in exchange for goods or services, they entered into implied contracts with Defendant.

201. Defendant entered into implied contracts with Plaintiff and the Class under which Defendant agreed to comply with its statutory and common law duties to safeguard and protect Plaintiff's and Class Members' Private Information and to timely notify Plaintiff and Class Members of a data breach. In exchange, Plaintiff and Class Members provided their Private Information to Defendant and paid money to Defendant, directly or indirectly, which a portion was to ensure that Defendant maintained adequate security measures to protect the PII of Plaintiff and the Class.

202. The implied promise of confidentiality includes consideration beyond those pre-existing duties owed under Section 5 of the FTC Act and other state and federal regulations. The additional consideration included implied promises to take adequate steps to comply with specific industry data security standards and FTC guidelines on data security.

203. The implied promises include, but are not limited to: (i) taking steps to ensure any agents or vendors who are granted access to Private Information protect the confidentiality of that information; (ii) taking steps to ensure that Private Information in the possession and control of Defendant, its agents, and/or vendors is restricted and limited to achieve an authorized business purpose; (iii) restricting access to qualified and trained agents and/or vendors; (iv) designing and implementing appropriate retention policies to protect the Private Information from unauthorized access and disclosure; (v) applying or requiring proper encryption of the Private Information; (vi) requiring multifactor authentication for access to the Private Information; and (vii) other steps necessary to protect against foreseeable data breaches.

204. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of such implied contracts.

205. Defendant recognized that Plaintiff's and Class Members' Private Information is highly sensitive and must be protected, and that this protection was of material importance to Plaintiff and Class Members.

206. Had Defendant disclosed to Plaintiff and Class Members that it did not have adequate data security practices to secure their Private Information, Plaintiff and Class Members would not have provided their Private Information to Defendant.

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

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

209. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiff and Class Members have suffered damages, including foreseeable consequential damages that Defendant knew about when they solicited and collected Plaintiff's and Class Members' Private Information.

210. Plaintiff and the Class have suffered injuries as described above, and are entitled to actual and punitive damages, statutory damages, and reasonable attorneys' fees and costs, in an amount to be proven at trial.

THIRD CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

211. Plaintiff re-alleges and incorporates by reference paragraphs 1-151 as if fully restated here.

212. Plaintiff alleges this claim in the alternative to her breach of implied contract claim.

213. Plaintiff and the Class provided their Private Information to Defendant in order to receive services or employment.

214. By conferring their Private Information to Defendant, Plaintiff and Class Members reasonably understood Defendant would be responsible for securing their Private Information from unauthorized access and disclosure.

215. Upon information and belief, Defendant funds its data security measures entirely from their general revenue, including from money it makes based on protecting Plaintiff's and Class Members' Private Information.

216. Plaintiff and Class Members paid Defendant, directly or indirectly, a certain sum of money, which was used to fund data security via contracts with Defendant

217. As such, a portion of the payments made by or on behalf of Plaintiff and the Class was to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

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

219. Protecting the Private Information of Plaintiff and Class Members is integral to Defendant's business. Without their Private Information, Defendant would be unable to provide

services comprising Defendant's core business.

220. Plaintiff's and Class Members' Private Information have monetary value.

221. Plaintiff and Class Members directly conferred a monetary benefit on Defendant by supplying their Private Information, from which Defendant derives its business, and which should have been protected with adequate data security.

222. Defendant solicited, collected, stored, and maintained Plaintiff's and Class Members' Private Information, and as such, Defendant had direct knowledge of the monetary benefits conferred upon it by Plaintiff and the Class. Defendant profited from these transactions and used Plaintiff's and Class Members' Private Information for business purposes.

223. Indeed, Plaintiff and Class Members who were customers of Defendant provided monetary payment to Defendant and therefore conferred a benefit unto Defendant.

224. Defendant appreciated that a monetary benefit was being conferred upon them by Plaintiff and Class Members and accepted that monetary benefit.

225. Under the facts and circumstances outlined above, however, it is inequitable for Defendant to retain that benefit without payment of the value thereof.

226. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Private Information.

227. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profits to the detriment of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite data security.

228. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary benefit belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures.

229. Defendant acquired Plaintiff's and Class Members' Private Information through inequitable means in that they failed to disclose their inadequate data security practices, as previously alleged.

230. If Plaintiff and Class Members knew that Defendant had not secured their Private Information, they would not have allowed Defendant to collect their Private Information.

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

232. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered or will suffer injury, including, but not limited to: (i) actual identity theft and fraud; (ii) loss of the opportunity to control how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, fraud, and/or unauthorized use of their Private Information; (v) lost time and opportunity costs associated with efforts to mitigate the actual and future consequences of the Data Breach, including, but not limited to, effort and time spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remains 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 Private Information in their continued possession; and/or (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

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

234. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, all gains that it unjustly received.

FOURTH CAUSE OF ACTION
DECLATORY AND INJUNCTIVE RELIEF
(On Behalf of Plaintiff and the Class)

235. Plaintiff re-alleges and incorporates by reference paragraphs 1-151 as if fully restated here.

236. This count is brought under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

237. As previously alleged, Plaintiff and members of the Class entered into implied contracts with Defendant, which contracts required Defendant to provide adequate security for the protection of the Private Information Defendant collected from Plaintiff and the Class.

238. Defendant owed and still owes a duty of care to Plaintiff and Class Members that require it to adequately secure Plaintiff's and Class Members' Private Information.

239. Upon information and belief, Defendant still possesses Plaintiff's and Class Members' Private Information.

240. Defendant has not satisfied its contractual obligations and legal duties to Plaintiff and Class Members.

241. Since the Data Breach, Defendant has not announced any changes to its data security infrastructure, processes or procedures to fix the vulnerabilities in its computer systems and/or security practices which permitted the Data Breach to occur and go undetected and, thereby, prevent further attacks.

242. Defendant has not satisfied its contractual obligations and legal duties to Plaintiff and the Class. In fact, now that Defendant's insufficient data security is known to hackers, the Private Information in Defendant's possession is even more vulnerable to cyberattacks.

243. Further, Plaintiff and Class Members are at risk of additional or further harm due to the exposure of their Private Information and Defendant's failure to address the security failings that led to such exposure.

244. There is no reason to believe that Defendant's security measures are any more adequate now than they were before the Data Breach.

245. Plaintiff and the Class, therefore, seek a declaration (1) that Defendant's existing security measures do not comply with their contractual obligations and duties of care to provide adequate security, and (2) that to comply with their contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

a. Ordering that Defendant engage third-party security auditors and 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;

b. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures;

d. Ordering that Defendant segment customer and employee data by, among other things, creating firewalls and access controls so that if one area of Defendant's systems 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, customer and employee data not necessary for their provisions of services;

f. Ordering that Defendant conduct regular database scanning and security checks; and

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.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff and the Class pray for judgment against Defendant as follows:

a. For an order determining that this action is properly brought as a class action and certifying Plaintiff as the representative of the Class and her counsel as Class Counsel;

b. A judgment in favor of Plaintiff and the Class awarding them appropriate monetary relief, including compensatory damages, punitive damages, attorney fees, expenses, costs, and such other and further relief as is just and proper;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d. An order requiring Defendant to pay the costs involved in notifying the Class Members about the judgment and administering the claims process;

e. A judgment in favor of Plaintiff and the Class awarding them pre-judgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

f. An award of such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on any and all issues raised in this Class Action Complaint so triable as of right.

Dated: August 7, 2026

Respectfully submitted,

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

Counsel for Plaintiff and Putative Class