UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO

DEVIN GIRTIN, individually and on behalf of all others similarly situated, Plaintiff, v. SM ENERGY COMPANY, Defendant.	**Case No.:** **COMPLAINT – CLASS ACTION** **JURY TRIAL DEMANDED**

Plaintiff, Devin Girtin ("Plaintiff"), on behalf of all others similarly situated, by and through his undersigned counsel, brings this Class Action Complaint against SM Energy Company ("Defendant"). Plaintiff alleges the following upon information and belief based on and the investigation of counsel, except as to those allegations that specifically pertain to Plaintiff, which are alleged upon personal knowledge.

INTRODUCTION

1. Plaintiff and the proposed Class Members bring this class action lawsuit on behalf of all persons who entrusted Defendant with sensitive Personally Identifiable Information ("PII")[1] including names and Social Security numbers (collectively "Private Information") that was impacted in a data breach that Defendant experienced on May 15, 2026 (the "Data Breach" or the "Breach").

[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.

2. Plaintiff's claims arise from Defendant's failure to properly secure and safeguard Private Information that was entrusted to it, and its accompanying responsibility to store and transfer that information.

3. Defendant is an oil and gas exploration company whose strategy is to focus on high quality, Lower 48 and natural gas producing assets, with top-tier economic drilling, completion, and production opportunities.[2]

4. Defendant had numerous statutory, regulatory, contractual, and common law duties and obligations, including those based on its affirmative representations to Plaintiff and Class Members, to keep their Private Information confidential, safe, secure, and protected from unauthorized disclosure or access.

5. Defendant claims that an unauthorized actor gained access to its systems and acquired the Private Information on May 15, 2026.[3]

6. On June 30, 2026, Defendant determined that Plaintiff's Private Information was exposed in the Data Breach.[4]

7. Defendant's investigation determined that the Private Information compromised in the Data Breach included individuals' names, postal addresses, emails, phone numbers, Social Security numbers, and Taxpayer Identification Numbers.[5]

8. On July 30, 2026, Defendant began sending out notice letters to individuals impacted notifying them of the Data Breach.[6]

---

[2] *See* https://www.sm-energy.com/about-us/fact-sheet (last visited Aug. 5, 2026).
[3] *See* Sample Notice, attached as **Exhibit A**.
[4] *Id.*
[5] *Id.*
[6] *Id.*

9. Defendant failed to take precautions designed to keep individuals' Private Information secure.

10. Defendant owed Plaintiff and Class Members a duty to take all reasonable and necessary measures to keep the Private Information it collected safe and secure from unauthorized access. Defendant solicited, collected, used, and derived a benefit from the Private Information, yet breached its duty by failing to implement or maintain adequate security practices.

11. Defendant admits that information in its system was accessed by unauthorized individuals, though it provided little information regarding how the Data Breach occurred.

12. The sensitive nature of the data exposed through the Data Breach signifies that Plaintiff and Class Members have suffered irreparable harm. Plaintiff and Class Members have lost the ability to control their private information and are subject to an increased risk of identity theft.

13. Defendant, despite having the financial wherewithal and personnel necessary to prevent the Data Breach, nevertheless failed to use reasonable security procedures and practice appropriate to the nature of the sensitive, unencrypted information it maintained for Plaintiff and Class Members, causing the exposure of Plaintiff's and Class Members' Private Information.

14. As a result of Defendant's inadequate digital security and notice process, Plaintiff's and Class Members' Private Information was exposed to criminals. Plaintiff and the Class Members have suffered and/or will suffer injuries including (1) financial losses caused by misuse of their Private Information; (2) the loss or diminished value of their Private Information as a result of the Data Breach; (3) lost time associated with detecting and preventing identity theft; and (4) theft of personal and financial information.

15. Upon information and belief, Plaintiff's Private Information is available on the Dark Web as a result of the Data Breach.

16. Plaintiff brings this action on behalf of all persons whose Private Information was compromised as a result of Defendant's failure to: (i) adequately protect the Private Information of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of Defendant's inadequate information security practices; (iii) effectively secure hardware containing protected Private Information using reasonable and adequate security procedures free of vulnerabilities and incidents; and (iv) timely notify Plaintiff and Class Members of the Data Breach.

17. Plaintiff brings this action individually and on behalf of a Nationwide Class of similarly situated individuals against Defendant for: negligence; negligence *per se*; unjust enrichment, breach of implied contract, and breach of confidence.

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

PARTIES

19. Plaintiff is a citizen and resident of Lakewood, Colorado.

20. Defendant is a Delaware corporation with its headquarters and principal place of business located at 1700 Lincoln Street, Suite 3200, Denver, CO 80203.

JURISDICTION AND VENUE

21. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. The number of class members is more than 100 and at least one member of the Class is a

citizen of a different state that is diverse from Defendant's citizenship. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

22. This Court has personal jurisdiction over Defendant because Defendant is registered to do business and maintains its principal place of business in this District.

23. Venue is proper in this Court because Defendant's principal place of business is located in this District, and because a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

FACTUAL ALLEGATIONS

Plaintiff

A. Background on Defendant

24. Defendant is an oil and gas exploration company whose strategy is to focus on high quality, Lower 48 and natural gas producing assets, with top-tier economic drilling, completion, and production opportunities.

25. Plaintiff and Class Members provided their Private Information to Defendant as a condition of receiving employment from Defendant.

26. Upon information and belief, Defendant made promises and representations to individuals, including 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.

27. Plaintiff and Class Members provided their Private Information 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.

28. Upon information and belief, in the course of collecting Private Information from Plaintiff and Class Members, Defendant promised to provide confidentiality and adequate security for the data it collected from Plaintiff and Class members through its applicable privacy policy and through other disclosures in compliance with statutory privacy requirements.

29. 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.

B. The Data Breach

30. On or around May 15, 2026, an unauthorized actor accessed and exfiltrated Private Information from Defendant's systems.[7]

31. On June 30, 2026, Defendant determined that the Private Information compromised in the Data Breach included individuals' names, postal addresses, emails, phone numbers, Social Security numbers, and Taxpayer Identification Numbers.[8]

32. On July 30, 2026, Defendant began sending out Notice of Data Breach letters ("Notice") to individuals impacted notifying them of the Data Breach.[9]

33. To be clear, there are numerous issues with Defendant's Data Breach, but the deficiencies in the Data Breach Notice exacerbate the circumstances for victims of the Data Breach: (1) Defendant fails to state whether it was able to contain or end the cybersecurity threat, leaving victims to fear whether the Private Information that Defendant continues to maintain is secure; (2) Defendant fails to state how the Breach itself occurred; (3) Defendant fails to state the

[7] Ex. A.
[8] *Id.*
[9] *Id.*

date on which the Breach was discovered; (4) Defendant fails to state whether it hired a third-party cybersecurity and cyber forensics expert to evaluate its systems and the extent of the data effected in the Breach; and (5) Defendant failed to notify victims until almost *two* months after the Breach occurred, depriving victims of the earliest opportunity to take preventative measures to protect their Private Information. All of this information is vital to victims of a data breach, let alone a data breach of this magnitude due to the sensitivity and wide array of information compromised in this specific breach.

34. Despite Defendant's intentional opacity about the root cause of this incident, several facts may be gleaned from the Notice, including: a) that this Data Breach was the work of cybercriminals; b) that the cybercriminals first infiltrated Defendant's networks and systems, and downloaded data from the networks and systems (aka exfiltrated data, or in layperson's terms "stole" data; and c) that once inside Defendant's networks and systems, the cybercriminals targeted information including Plaintiff's and Class Members' Private Information and other sensitive information for download and theft.

35. Moreover, in its Notice, Defendant failed to specify whether it undertook any efforts to contact the Class Members whose data was accessed and acquired in the Data Breach to inquire whether any of the Class Members suffered misuse of their data, whether Class Members should report their misuse to Defendant, and whether Defendant set up any mechanism for Class Members to report any misuse of their data.

36. Defendant failed to take precautions designed to keep individuals' Private Information secure.

37. While Defendant sought to minimize the damage caused by the Data Breach, it cannot and has not denied that there was unauthorized access to the sensitive Private Information of Plaintiff and Class Members.

38. Individuals affected by the Data Breach are, and remain, at risk that their data will be sold or listed on the dark web and, ultimately, illegally used in the future.

39. Plaintiff further believes that the Private Information 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.

C. Data Breaches Are Preventable

40. Defendant could have prevented this Data Breach by, among other things, properly encrypting or otherwise protecting their equipment and computer files containing Private Information.

41. 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."[10]

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

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.

- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

[10] How to Protect Your Networks from RANSOMWARE, at 3, *available at:* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited Aug. 5, 2026).

- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[11]

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

[11] *Id.* at 3-4.

Secure internet-facing assets

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

Thoroughly investigate and remediate alerts

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

Include IT Pros in security discussions

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

Build credential hygiene

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

Apply principle of least-privilege

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

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[12]

44. Given that Defendant was storing the sensitive Private Information of Plaintiff and Class Members, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

[12] See Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), available at: https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited Aug. 5, 2026).

45. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the Private Information of, upon information and belief, hundreds, and possibly thousands of individuals, including that of Plaintiff and Class Members.

D. Defendant Acquires, Collects, and Stores Plaintiff's and Class Members' Private Information

46. Plaintiff and Class Members were required to give their sensitive and confidential Private Information to Defendant as a condition of receiving employment.

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

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

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

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

51. Upon information and belief, Defendant made promises to Plaintiff and Class Members to maintain and protect their Private Information, demonstrating an understanding of the importance of securing Private Information.

52. Defendant's negligence in safeguarding the Private Information of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

E. The Data Breach Was Foreseeable and the Defendant Was Aware of Its Risk

53. It is well known that Private Information, including names and Social Security numbers in particular are invaluable commodities and a frequent target of hackers.

54. In 2024, a 3,158 data breaches occurred, exposing approximately 1,350,835,988 sensitive records—a 211% increase year-over-year.[13]

55. Individuals place a high value not only on their Private Information, but also on the privacy of that data. For the individual, identity theft causes "significant negative financial impact on victims" as well as severe distress and other strong emotions and physical reactions.

56. In light of recent high profile data breaches at other industry-leading companies, including, *e.g.*, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or should have known that the Private Information that it collected and maintained would be targeted by cybercriminals.

57. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of and take appropriate measures to prepare for and are able to thwart such an attack.

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

---

[13] ITRC (Identity Theft Resource Center), *2024 Data Breach Report* (January 2025), *available at* https://www.idtheftcenter.org/publication/2024-data-breach-report/ (last accessed Aug. 5, 2026).

59. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's server(s), and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

60. In the Notice, Defendant makes an offer of identity monitoring services. This is wholly inadequate to compensate Plaintiff and Class Members as it fails to provide for the fact victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft, financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiff and Class Members' Private Information. Moreover, once this service expires, Plaintiff and Class Members will be forced to pay out of pocket for necessary identity monitoring services. [14]

61. Defendant's offering of credit and identity monitoring establishes that Plaintiff and Class Members' sensitive Private Information *was* in fact affected, accessed, compromised, and exfiltrated from Defendant's computer systems.

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

63. The ramifications of Defendant's failure to keep secure the Private Information of Plaintiff and Class Members are long lasting and severe. Once Private Information is stolen fraudulent use of that information and damage to victims may continue for years.

64. As an entity in possession of Plaintiff's and Class Members' Private Information, Defendant knew, or should have known, the importance of safeguarding the Private Information entrusted to it by Plaintiff and Class Members and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiff and Class Members because of a breach. Nevertheless, Defendant failed to take adequate cybersecurity measures to prevent the Data Breach.

---

[14] *Id.*

F. Defendant Fails to Comply with FTC Guidelines

65. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

66. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal customer 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 to correct any security problems.[15]

67. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[16]

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

69. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15

---

[15] *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (2016), https://ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed Aug. 5, 2026).
[16] *Id.*

U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

70. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect Private Information.

71. Defendant failed to properly implement basic data security practices.

72. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' Private Information or to comply with applicable industry standards constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

73. Upon information and belief, Defendant was at all times fully aware of its obligation to protect the Private Information of Plaintiff and Class Members; Defendant was also aware of the significant repercussions that would result from its failure to do so. Accordingly, Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class Members.

G. Defendant Fails to Comply with Industry Standards

74. As noted above, experts studying cyber security routinely identify companies in possession of Private Information as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

75. Several best practices have been identified that, at a minimum, should be implemented by companies in possession of Private Information, like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data.

Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

76. Other best cybersecurity practices that are standard include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

77. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

78. These foregoing frameworks are existing and applicable industry standards for safeguarding data, and upon information and belief, Defendant failed to comply with at least one––or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

H. Defendant Owed Plaintiff and Class members a Duty to Safeguard their Private Information

79. In addition to its obligations under federal and state laws, Defendant owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the Private Information of Class Members.

80. Defendant owed a duty to Plaintiff and Class Members to create and implement reasonable data security practices and procedures to protect the Private Information in its possession, including adequately training its employees and others who accessed Private Information within its computer systems on how to adequately protect Private Information.

81. Defendant owed a duty to Plaintiff and Class Members to implement processes that would detect a compromise of Private Information in a timely manner.

82. Defendant owed a duty to Plaintiff and Class Members to act upon data security warnings and alerts in a timely fashion.

83. Defendant owed a duty to Plaintiff and Class Members to disclose in a timely and accurate manner when and how the Data Breach occurred.

84. Defendant owed a duty of care to Plaintiff and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

I. The Harm Caused by the Data Breach Now and Going Forward

85. Victims of data breaches are susceptible to becoming victims of identity theft. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 17 C.F.R. § 248.201(9). When "identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance."[17]

86. The type of data that may have been accessed and compromised here can be used to perpetrate fraud and identity theft.

87. Plaintiff and Class Members face a substantial risk of identity theft given that their Private Information was compromised in the Data Breach.

88. Stolen Private Information is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines. Law enforcement

[17] *Prevention and Preparedness*, New York State Police, https://troopers.ny.gov/prevention-and-preparedness_ (last visited Aug. 5, 2026).

has difficulty policing the "dark web" due to this encryption, which allows users and criminals to conceal their identities and online activity.

89. When malicious actors infiltrate companies and copy and exfiltrate the Private Information that those companies store, the stolen information often ends up on the dark web where malicious actors buy and sell that information for profit.[18]

90. For example, when the U.S. Department of Justice announced their seizure of AlphaBay—the largest online "dark market"—in 2017, AlphaBay had more than 350,000 listings, many of which concerned stolen or fraudulent documents that could be used to assume another person's identity."[19] Marketplaces similar to the now-defunct AlphaBay continue to be "awash with [PII] belonging to victims from countries all over the world."[20]

91. PII remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[21] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[22]

---

[18] *Shining a Light on the Dark Web with Identity Monitoring*, IDENTITYFORCE (Dec. 28, 2020) https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring (last visited Aug. 5, 2026).

[19] *Stolen PII & Ramifications: Identity Theft and Fraud on the Dark Web*, ARMOR (April 3, 2018), https://res.armor.com/resources/blog/stolen-pii-ramifications-identity-theft-fraud-dark-web/ (last visited Aug. 5, 2026).

[20] *Id.*

[21] *Id.*

[22] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015) https://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited Aug. 5, 2026).

92. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses in 2019, resulting in more than $3.5 billion in losses to individuals and business victims.[23]

93. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[24] Defendant did not rapidly report to Plaintiff and Class Members that their Private Information had been stolen. Defendant waited almost two months after the Data Breach to notify impacted people.

94. As a result of the Data Breach, the Private Information of Plaintiff and Class Members has been exposed to criminals for misuse. The injuries suffered by Plaintiff and Class Members, or likely to be suffered as a direct result of Defendant's Data Breach, include: (a) theft of their Private Information; (b) costs associated with the detection and prevention of identity theft; (c) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the consequences of this Breach; (d) invasion of privacy; (e) the emotional distress, stress, nuisance, and annoyance of responding to, and resulting from, the Data Breach; (f) the actual and/or imminent injury arising from actual and/or potential fraud and identity theft resulting from their personal data being placed in the hands of the ill-intentioned hackers and/or criminals; (g) damage to and diminution in value of their personal data entrusted to Defendant with the mutual understanding that Defendant would safeguard their Private Information against theft and not allow access to and misuse of their personal data by any unauthorized third party; and (h) the continued risk to their Private Information, which remains in the possession of Defendant, and which is subject to further injurious breaches so long as

---

[23] *2019 Internet Crime Report Released*, FBI (Feb. 11, 2020) https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120#:~:text=IC3%20received%20467%2C361%20complaints%20in,%2Ddelivery%20scams%2
C%20and%20extortion (last visited Aug. 5, 2026).

[24] *Id.*

Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information.

95. In addition to a remedy for economic harm, Plaintiff and Class Members maintain an interest in ensuring that their Private Information is secure, remains secure, and is not subject to further misappropriation and theft.

96. Defendant disregarded the rights of Plaintiff and Class Members by (a) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that its network servers were protected against unauthorized intrusions; (b) failing to disclose that it did not have adequately robust security protocols and training practices in place to safeguard Plaintiff's and Class Members' Private Information; (c) failing to take standard and reasonably available steps to prevent the Data Breach; and (d) failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach.

97. The actual and adverse effects to Plaintiff and Class Members, including the imminent, immediate, and continuing increased risk of harm for identity theft and identity fraud directly or proximately caused by Defendant's wrongful actions and/or inaction and the resulting Data Breach require Plaintiff and Class Members to take affirmative acts to recover their peace of mind and personal security including, without limitation, purchasing credit reporting services, purchasing credit monitoring and/or internet monitoring services, frequently obtaining, purchasing and reviewing credit reports, bank statements, and other similar information, instituting and/or removing credit freezes and/or closing or modifying financial accounts, for which there is a financial and temporal cost. Plaintiff and other Class Members have suffered, and will continue to suffer, such damages for the foreseeable future.

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

98. 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.

99. In fact, Defendant in its Notice instructs Plaintiff and Class Members to "be vigilant for incidents of fraud or identity theft by reviewing account statements and free credit reports for any unauthorized activity."[25]

100. Thus, due to the actual and imminent risk of identity theft, Plaintiff and Class Members must monitor their financial accounts for many years to mitigate the risk of identity theft.

101. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as changing passwords and resecuring their own computer systems.

102. Plaintiff's mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[26]

103. Plaintiff's mitigation efforts are also consistent with the steps the FTC recommends data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (and considering 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.[27]

---

[25] Ex. A.

[26] *See* United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf (last accessed Aug. 5, 2026).

[27] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps (last accessed Aug. 5, 2026).

104. And for those Class Members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."

K. Diminution of Value of Private Information

105. Private Information is valuable property.[28] Its value is axiomatic, considering the value of Big Data in corporate America and that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk-to-reward analysis illustrates, beyond doubt, that Private Information has considerable market value.

106. The Private Information stolen in the Data Breach is significantly more valuable than the loss of, say, credit card information in a large retailer data breach. Victims affected by those retailer breaches could avoid much of the potential future harm by simply cancelling credit or debit cards and obtaining replacements. The information stolen in the Data Breach is difficult, if not impossible, to change – name and Social Security number.

107. This kind of data, as one would expect, demands a much higher price on the dark web. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information . . . [is] worth more than 10x on the black market."[29]

108. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[30]

---

[28] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," at 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last accessed Aug. 5, 2026) ("GAO Report").

[29] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT WORLD (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hackpersonal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed Aug. 5, 2026).

[30] *See, e.g.*, John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("Private Information") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech.

109. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[31] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[32,33] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50 a year.[34]

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

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

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

11, at *3-4 (2009) ("Private Information, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[31] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last accessed Aug. 5, 2026).

[32] https://Riverbay.latimes.com/business/story/2019-11-05/column-data-brokers (last accessed October 15, 2025).

[33] https://datacoup.com/ (last accessed Aug. 5, 2026).

[34] https://www.thepennyhoarder.com/make-money/nielsen-panel/#:~:text=Sign%20up%20to%20join%20the,software%20installed%20on%20your%20computer (last accessed Aug. 5, 2026)

113. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, amounting to hundreds, and possibly thousands of individuals who would be harmed by the exposure of the unencrypted data.

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

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

115. Given the type of targeted attack in this case, the sophisticated criminal activity, the volume of data compromised in this Data Breach, and the sensitive type of Private Information involved in this Data Breach, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/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; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

116. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Private 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.

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

118. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is a reasonable and necessary cost to monitor and protect Class Members from the risk of identity theft resulting 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.

M. Loss of the Benefit of the Bargain

119. Furthermore, Defendant's poor data security deprived Plaintiff and Class Members of the benefit of their bargain. When agreeing to provide their Private Information, Plaintiff and other reasonable Class Members understood and expected that they were, in part, exchanging their Private Information for Defendant's services and necessary data security to protect the Private Information when, in fact, Defendant did not provide the expected data security. Accordingly, Plaintiff and Class Members received services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

Plaintiff's Experience

120. Plaintiff is a former employee of Defendant.

121. As a condition of obtaining employment from Defendant, Plaintiff was required to provide Defendant with his Private Information.

122. Defendant was in possession of Plaintiff's Private Information before, during and after the Data Breach.

123. Plaintiff reasonably understood and expected that Defendant would safeguard his Private Information and timely and adequately notify him in the event of a data breach. Plaintiff would not have allowed Defendant, or anyone in Defendant's position, to maintain his Private Information if he believed that Defendant would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

124. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff faces, Defendant offered victims of the Data Breach a temporary subscription to a credit monitoring service via the notice letter sent to impacted individuals.

125. Plaintiff greatly values his privacy and Private Information and takes reasonable steps to maintain the confidentiality of his Private Information. Plaintiff is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud that he is at an increased risk of experiencing, as a result of the Data Breach.

126. Plaintiff stores any and all documents containing Private Information in a secure location and destroys any documents he receives in the mail that contain any Private Information or that may contain any information that could otherwise be used to compromise his identity and credit card accounts. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

127. As a result of the Data Breach, Plaintiff has spent several hours researching the Data Breach, reviewing his bank accounts, monitoring his credit report, changing his passwords and other necessary mitigation efforts. This is valuable time that Plaintiff spent at Defendant's direction and that he otherwise would have spent on other activities, including but not limited to work and/or recreation.

128. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant's notice did not include all relevant details about the Data Breach, other than noticing him of the fact that his Social Security number in conjunction with his name was acquired by criminals as a result of the Data Breach.

129. Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff will continue to be at present and continued increased risk of identity theft and fraud for years to come.

130. Plaintiff has a continuing interest in ensuring that his Private Information, which upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

131. As a direct and traceable result of the Data Breach, Plaintiff suffered actual injury and damages after his Private Information was compromised and stolen in the Data Breach, including, but not limited to: (a) lost time and money related to monitoring his accounts and credit reports for fraudulent activity; (b) loss of privacy due to his Private Information being accessed and stolen by cybercriminals; (c) loss of the benefit of the bargain because Defendant did not adequately protect his Private Information; (d) emotional distress because identity thieves now possess his first and last name paired with his Social Security number; (e) imminent and impending

injury arising from the increased risk of fraud and identity theft now that his Private Information has been stolen and likely published on the dark web; (f) diminution in the value of his Private Information, a form of intangible property that Defendant obtained from Plaintiff and (g) other economic and non-economic harm.

CLASS ALLEGATIONS

132. Plaintiff brings this class action, individually and on behalf of class defined as:

> **Nationwide Class**: All persons residing in the Unites Sates whose Private Information was impacted in the Data Breach (the "Class").

133. Specifically excluded from the Class are Defendant, its officers, directors, agents, trustees, parents, children, corporations, trusts, representatives, principals, servants, partners, joint venturers, or entities controlled by Defendant, and its heirs, successors, assigns, or other persons or entities related to or affiliated with Defendant and/or its officers and/or directors, the judge assigned to this action, and any member of the judge's immediate family.

134. Plaintiff reserves the right to amend the Class definition above if further investigation and/or discovery reveals that the Class should be expanded, narrowed, divided into subclasses, or otherwise modified in any way.

135. This action may be certified as a class action because it satisfies the numerosity, commonality, typicality, adequacy, and superiority requirements therein.

136. Numerosity: The Class is so numerous that joinder of all Class Members is impracticable. Although the precise number of such persons is unknown, and the facts are presently within the sole knowledge of Defendant, upon information and belief, Plaintiff estimates that the Class is comprised of hundreds, and possibly thousands of Class Members, if not more. The Class is sufficiently numerous to warrant certification.

137. Typicality of Claims: Plaintiff's claims are typical of those of other Class Members because Plaintiff, like the unnamed Class, had his Private Information compromised as a result of the Data Breach. Plaintiff is a member of the Class, and his claims are typical of the claims of the

members of the Class. The harm suffered by Plaintiff is similar to that suffered by all other Class Members which was caused by the same misconduct by Defendant.

138. Adequacy of Representation: Plaintiff will fairly and adequately represent and protect the interests of the Class. Plaintiff has no interests antagonistic to, nor in conflict with, the Class. Plaintiff has retained competent counsel who are experienced in consumer and commercial class action litigation and who will prosecute this action vigorously.

139. Superiority: A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Because the monetary damages suffered by individual Class Members are relatively small, the expense and burden of individual litigation make it impossible for individual Class Members to seek redress for the wrongful conduct asserted herein. If Class treatment of these claims is not available, Defendant will likely continue its wrongful conduct, will unjustly retain improperly obtained revenues, or will otherwise escape liability for its wrongdoing as asserted herein.

140. Predominant Common Questions: The claims of all Class Members present common questions of law or fact, which predominate over any questions affecting only individual Class Members, including:

a. 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;

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

c. Whether Defendant's storage of Plaintiff's and Class Member's Private Information was done in a negligent manner;

d. Whether Defendant had a duty to protect and safeguard Plaintiff's and Class Members' Private Information;

e. Whether Defendant's conduct was negligent;

f. Whether Defendant's conduct violated Plaintiff's and Class Members' privacy;

g. Whether Defendant took sufficient steps to individuals' Private Information;

h. Whether Defendant was unjustly enriched; and

i. The nature of relief, including damages and equitable relief, to which Plaintiff and Class Members are entitled.

141. Information concerning Defendant's policies is available from Defendant's records.

142. Plaintiff knows of no difficulty which will be encountered in the management of this litigation which would preclude its maintenance as a class action.

143. The prosecution of separate actions by individual members of the Class would run the risk of inconsistent or varying adjudications and establish incompatible standards of conduct for Defendant.

144. Prosecution as a class action will eliminate the possibility of repetitious and inefficient litigation.

145. Given that Defendant has not indicated any changes to its conduct or security measures, monetary damages are insufficient and there is no complete and adequate remedy at law.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

146. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above in paragraphs 1 through 145 as though fully set forth herein.

147. Plaintiff brings this claim individually and on behalf of the Class Members.

148. Defendant knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

149. Defendant had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiff's and Class Members' Private Information.

150. Defendant had, and continues to have, a duty to timely disclose that Plaintiff's and Class Members' Private Information within its possession was compromised and precisely the types of information that were compromised.

151. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards, applicable standards of care from statutory authority like Section 5 of the FTC Act, and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected individuals' Private Information.

152. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and Class members. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Plaintiff and Class Members from a data breach.

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

154. Defendant breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' Private Information.

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

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

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

c. Failing to periodically ensure that its computer systems and networks had plans in place to maintain reasonable data security safeguards.

156. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' Private Information within Defendant's possession.

157. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiff's and Class Members' Private Information.

158. Defendant, through its actions and/or omissions, unlawfully breached its duty to timely disclose to Plaintiff and Class Members that the Private Information within Defendant's possession might have been compromised and precisely the type of information compromised.

159. Defendant breached the duties set forth in 15 U.S.C. § 45, the FTC guidelines, the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity, and other industry guidelines. In violation of 15 U.S.C. § 45, Defendant failed to implement proper data security procedures to adequately and reasonably protect Plaintiff's and Class Members' Private Information. In violation of the FTC guidelines, *inter alia,* Defendant did not protect the Private Information it keeps; failed to properly dispose of personal information that was no longer needed; failed to encrypt information stored on computer networks; lacked the requisite understanding of its networks' vulnerabilities; and failed to implement policies to correct security issues.

160. 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. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches.

161. It was foreseeable that the failure to adequately safeguard Plaintiff's and Class Members' Private Information would result in injuries to Plaintiff and Class Members.

162. Defendant's breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' Private Information to be compromised.

163. But for Defendant's negligent conduct and breach of the above-described duties owed to Plaintiff and Class Members, their Private Information would not have been compromised.

164. As a result of Defendant's negligence and breach of duties, Plaintiff and Class Members are in danger of imminent harm in that their Private Information, which is still in the

possession of third parties, will be used for fraudulent purposes, and Plaintiff and Class Members have and will suffer damages including: a substantial increase in the likelihood of identity theft; the compromise, publication, and theft of their personal information; loss of time and costs associated with the prevention, detection, and recovery from unauthorized use of their personal information; the continued risk to their personal information; future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the personal information compromised as a result of the Data Breach.

COUNT II
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class)

165. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above in paragraphs 1 through 145 as though fully set forth herein.

166. Section 5 of the FTC Act, 15 U.S.C. 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by Defendant of failing to use reasonable measures to protect Plaintiff's and Class Members' Private Information. Various FTC publications and orders also form the basis of Defendant's duty.

167. Defendant violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Plaintiff's and Class Members' Private Information and by failing to comply with industry standards.

168. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information obtained and stored and the foreseeable consequences of a data breach on Defendant's systems.

169. Class Members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes) were intended to protect.

170. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security

measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class Members.

171. As a result of Defendant's negligence *per se*, Plaintiff and Class Members have been harmed and have suffered damages including, but not limited to: damages arising from identity theft and fraud; out-of-pocket expenses associated with procuring identity protection and restoration services; increased risk of future identity theft and fraud, and the costs associated therewith; and time spent monitoring, addressing, and correcting the current and future consequences of the Data Breach.

COUNT III
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

172. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above in paragraphs 1 through 145 as though fully set forth herein.

173. Plaintiff and Class Members conferred a benefit upon Defendant by providing Defendant with their Private Information.

174. Defendant appreciated or had knowledge of the benefits conferred upon itself by Plaintiff. Defendant also benefited from the receipt of Plaintiff's and Class Members' Private Information.

175. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff's and the Class Members' Private Information because Defendant failed to adequately protect their Private Information. Plaintiff and the proposed Class would not have provided their Private Information to Defendant had they known Defendant would not adequately protect their Private Information.

176. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds received by it because of its misconduct and the Data Breach it caused.

COUNT IV
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)

177. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above in paragraphs 1 through 145 as though fully set forth herein.

178. Plaintiff and the Class provided and entrusted their Private Information to Defendant. Plaintiff and the Class provided their Private Information to Defendant as part of Defendant's regular business practices.

179. In so doing, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen, in return for seeking employment and/or services from Defendant. Implied in these exchanges was a promise by Defendant to ensure that the Private Information of Plaintiff and Class Members in its possession was secure.

180. Pursuant to these implied contracts, Plaintiff and Class Members provided Defendant with their Private Information. In exchange, Defendant agreed to, among other things, and Plaintiff and the Class understood that Defendant would: (1) provide employment and/or services to Plaintiff and Class Members'; (2) take reasonable measures to protect the security and confidentiality of Plaintiff's and Class Members' Private Information; and (3) protect Plaintiff's and Class Members' Private Information in compliance with federal and state laws and regulations and industry standards and in accordance with Defendant's own internal privacy policy.

181. Implied in these exchanges was a promise by Defendant to ensure the Private Information of Plaintiff and Class Members in its possession was only used to provide the agreed-upon reasons, and that Defendant would take adequate measures to protect Plaintiff and Class Members' Private Information.

182. A material term of this contract is a covenant by Defendant that it would take reasonable efforts to safeguard that information. Defendant breached this covenant by allowing Plaintiff and Class Members' Private Information to be accessed in the Data Breach.

183. Indeed, implicit in the agreement between Defendant and Plaintiff and Class Members was the obligation that both parties would maintain information confidentially and securely.

184. These exchanges constituted an agreement and meeting of the minds between the parties.

185. When the parties entered into an agreement, mutual assent occurred. Plaintiff and Class Members would not have disclosed their Private Information to Defendant but for the prospect of seeking employment and/or business services from Defendant. Conversely, Defendant presumably would not have taken Plaintiff and Class Members' Private Information if it did not intend to provide services to Plaintiff and Class Members.

186. Defendant was therefore required to reasonably safeguard and protect the Private Information of Plaintiff and Class Members from unauthorized disclosure and use.

187. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of their implied contracts with Defendant and would have instead retained the opportunity to control their Private Information.

188. Defendant breached the implied contracts with Plaintiff and Class Members by failing to reasonably safeguard and protect Plaintiff and Class Members' Private Information.

189. Defendant's failure to implement adequate measures to protect the Private Information of Plaintiff and Class Members violated the purpose of the agreement between the parties.

190. As a proximate and direct result of Defendant's breaches of its implied contracts with Plaintiff and Class Members, Plaintiff and the Class Members suffered damages as described in detail above.

COUNT V
BREACH OF CONFIDENCE
(On Behalf of Plaintiff and the Class)

191. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above in paragraphs 1 through 145 as though fully set forth herein.

192. At all times during Plaintiff's and Class Members' interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and Class Members' Private Information that Plaintiff and Class Members entrusted to Defendant.

193. As alleged herein and above, Defendant's relationship with Plaintiff and the Class was governed by terms and expectations that Plaintiff's and the Class Members' Private Information would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

194. Plaintiff and the Class entrusted Defendant with their Private Information with the explicit and implicit understandings that Defendant would protect and not permit the Private Information to be disseminated to any unauthorized third parties.

195. Plaintiff and the Class also entrusted Defendant with their Private Information with the explicit and implicit understanding that Defendant would take precautions to protect that Private Information from unauthorized disclosure.

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

197. As a result of Defendant's failure to prevent and avoid the Data Breach from occurring, Plaintiff's and Class Members' Private Information was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and Class Members' confidence, and without their express permission.

198. As a direct and proximate cause of Defendant's actions and omissions, Plaintiff and the Class have suffered damages.

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

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

201. As a direct and proximate result of Defendant's breach of its confidence with Plaintiff and the Class, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) identity theft; (ii) the loss of the opportunity 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, tax fraud, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual present and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information of individuals; and (viii) present and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

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

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, seeks 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 his counsel as Class Counsel;

(b) For an order declaring that Defendant's conduct violates the laws referenced herein;

(c) For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

(d) For damages in amounts to be determined by the Court and/or jury;

(e) For an award of statutory damages or penalties to the extent available;

(f) For pre-judgment interest on all amounts awarded;

(g) For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

(h) For an order of restitution and all other forms of monetary relief; and

(i) Such other and further relief as the Court deems necessary and appropriate.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

[SIGNATURE BLOCK ON FOLLOWING PAGE]

Dated: August 5, 2026

By: */s/ Jeff Ostrow*
Jeff Ostrow
KOPELOWITZ OSTROW P.A.
One West Las Olas Blvd, Suite 500
Fort Lauderdale, FL 33301
Tel: (954) 525-4100
ostrow@kolawyers.com

Gary M. Klinger
MILBERG, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: 866.252.0878
Email: gklinger@milberg.com

Attorneys for Plaintiff and the Proposed Class