UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO

TODD W MADSEN, on behalf of himself and all others similarly situated, Plaintiff, v. CLARITY TELECOM, LLC d/b/a BLUEPEAK, Defendant.	Case No. 1:26-cv-2664 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiff, Todd W Madsen ("Plaintiff"), individually and on behalf of all others similarly situated, by and through his undersigned counsel, brings this Class Action Complaint against Clarity Telecom, LLC d/b/a Bluepeak ("Bluepeak" or "Defendant"). Plaintiff alleges the following upon information and belief based on the investigation of counsel, except as to those allegations that specifically pertain to Plaintiff, which are alleged upon personal knowledge.

INTRODUCTION

1. Plaintiff brings this class action lawsuit individually and on behalf of all persons who entrusted Defendant with sensitive Personally Identifiable Information ("PII")[1] and Protected Health Information ("PHI" and collectively with PII "Private

[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.

Information") who were impacted in a data breach Defendant experienced on or around December 2025 (the "Data Breach" or the "Breach").

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 a telecommunications and internet service provider that offers fiber internet, phone, and related communication services to residential and business customers in parts of South Dakota, Minnesota, Wyoming, Oklahoma, North Dakota, and Texas. Defendant is headquartered in Denver, Colorado.[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. On December 11, 2025, Defendant detected suspicious activity within the computer network.[3] Upon detection, Defendant promptly began an investigation, to determine the nature and scope of the incident.[4]

6. The investigation determined that an unauthorized third-party gained access to Defendant's network and obtained sensitive data between December 19, 2024 and December 22, 2024.[5]

7. Defendant then launched a comprehensive review of the incident to identify

[2] *About Us*, BLUEPEAK, https://mybluepeak.com/about-us/ (last visited June 15, 2026).
[3] *Exhibit 1:* Todd Madsen's Notice Letter
[4] *Id.*
[5] *Id.*

the exact type of information compromised as well as identify the individuals affected in the Data Breach.[6]

8. Upon information and belief, the following types of sensitive personal and protected health information may have been compromised in the Data Breach: names, government identifier and/or information affiliated with Defendant's employee health insurance program. [7]

9. On May 19, 2026, Defendant filed a notice of Data Breach with the office of the Texas Attorney General and started sending out notice letter to the affected individual.[8]

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

11. Defendant owed Plaintiff and Class Members a duty to take all reasonable and necessary measures to keep the Private Information 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.

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

---

[6] *Id.*
[7] *Id.*
[8] *Data Security Breach Reports: Clarity Telecom, LLC d/b/a Bluepeak*, OFFICE OF THE ATTORNEY GENERAL OF TEXAS, https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage (last visited June 15, 2026)

13. 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.

14. 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.

15. 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 Class Members have suffered and will continue to suffer injuries, including: financial losses caused by misuse of their Private Information; the loss or diminished value of their Private Information as a result of the Data Breach; lost time associated with detecting and preventing identity theft; and theft of personal and financial information.

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 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 Private Information 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

Plaintiff

19. Plaintiff, Todd W Madsen, is a natural person and citizen of South Dakota. He resides in Sturgis, South Dakota, where he intends to remain.

Defendant

20. Defendant is a telecommunications and internet service provider that offers fiber internet, phone, and related communication services to residential and business customers in parts of South Dakota, Minnesota, Wyoming, Oklahoma, North Dakota, and Texas. Defendant is a Delaware corporation, headquartered in Denver, Colorado, having its principal place of business located at 4600 S. Ulster Street, Suite 1300 Denver, Colorado 80237.[9]

JURISDICTION & 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

[9] *Contact Us,* BLUEPEAK, https://mybluepeak.com/support/contact-us/ (last visited June 15, 2026).

million, exclusive of interest and costs. The number of class members is more than 100, and at least one member of the Class defined below is a citizen of a different state that is diverse from Defendant's citizenship.[10] 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

A. Background on Defendant

24. Defendant is a telecommunications and internet service provider that offers fiber internet, phone, and related communication services to residential and business customers in parts of South Dakota, Minnesota, Wyoming, Oklahoma, North Dakota, and Texas. Defendant is headquartered in Denver, Colorado.[11]

25. 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.[12]

---

[10] *Data Security Breach Reports: Clarity Telecom, LLC d/b/a Bluepeak*, OFFICE OF THE ATTORNEY GENERAL OF TEXAS, https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage (last visited June 15, 2026).
[11] *About Us*, BLUEPEAK, https://mybluepeak.com/about-us/ (last visited June 15, 2026).
[12] *Exhibit 1:* Todd Madsen's Notice Letter

26. 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.

27. 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

28. As a condition of receiving fiber internet services from Defendant, Plaintiff provided Defendant with his Private Information, including but not limited to his name, address, date of birth, Social Security number and banking information to transmit payments. Defendant used that Private Information to facilitate its business, and required Plaintiff to provide that Private Information to obtain services.

29. On information and belief, Defendant collects and maintains its clients' unencrypted Private Information in its computer systems.

30. In collecting and maintaining the Private Information, Defendant implicitly agreed that it will safeguard the data using reasonable means according to its internal policy as well as state and federal law.

31. According to a letter Bluepeak submitted to the Massachusetts Office of Consumer Affairs and Business Regulation (the "Breach Notice")[13], Defendant states that

[13] *Id.*

December 11, 2025, it "detected suspicious activity" within its computer network.[14]

32. Bluepeak states that it conducted an investigation with the assistance of independent cybersecurity experts, which determined that "some of the computer files copied off our systems" contained its clients' Private Information.[15]

33. In other words, Bluepeak's investigation revealed Defendant's cyber and data security systems were completely inadequate and allowed cybercriminals to obtain and remove files containing a treasure trove of thousands of its clients' highly Private Information.

34. Through its inadequate security practices, Defendant exposed Plaintiff's and the Class's Private Information for theft and sale on the dark web.

35. Despite its duties to safeguard Private Information, Defendant did not in fact follow industry standard practices in securing its clients' Private Information, as evidenced by the Data Breach.

36. In response to the Data Breach, Defendant contends that it has "taken steps to reinforce our computer network through the implementation of additional security measures."[16] Though Defendant fails to expand on what those "measures" are, such steps should have been in place before the Data Breach.

37. Through its Breach Notice, Defendant recognized the actual imminent harm and injury that flowed from the Data Breach, warning Data Breach victims to "monitor your credit reports for any activity you do not recognize," and to place fraud alerts and/or

[14] *Id.*
[15] *Id.*
[16] *Id.*

freezes on their credit files.[17]

38. Moreover, Defendant's statements that it "detected suspicious activity" on its computer network and that its clients' Private Information was "copied" indicates that Defendant experienced a ransomware attack.

39. According to the United States Cybersecurity and Infrastructure Security Agency ("CISA"), ransomware is a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Thereafter, the cybercriminals demand a ransom payment in exchange for decryption, often threatening to sell or leak exfiltrated data if the ransom is not paid.

40. Defendant has made no public statements regarding whether it experienced a ransomware attack or whether it made a ransom payment.

41. However, even if Defendant made a ransom payment, there is no guarantee that the Private Information stolen in the Data Breach will be deleted. The stolen Private Information is valuable, and can easily be sold to another threat actor, so there is little incentive to delete it.

42. Thus, on information and belief, Plaintiff's and the Class's stolen Private Information has already been published—or will be published imminently—by cybercriminals on the dark web.

43. Upon information and belief, Defendant has offered complimentary credit monitoring services to Data Breach victims. However, this does not adequately address the lifelong harm that victims will face following the Data Breach. Indeed, the breach

[17] *Id.*

involves Private Information that cannot be changed, such as Social Security numbers.

44. Even with several months of credit monitoring services, the risk of identity theft and unauthorized use of Plaintiff's and Class Members' Private Information is still substantially high. The fraudulent activity resulting from the Data Breach may not come to light for years.

45. On information and belief, Defendant failed to adequately train its IT and data security employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over its clients' Private Information. Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from stealing the Private Information.

46. On or around May 7, 2026—5 months after Defendant detected the Data Breach—Defendant reported the breach to some state attorney's general and sent a letter to some breach victims notifying them about the Data Breach.[18]

47. Defendant's delayed notice kept the Class in the dark—thereby depriving the Class of the opportunity to try and mitigate their injuries in a timely manner.

48. Moreover, Defendant's Breach Notice was completely inadequate—refusing to tell victims how the breach happened, when it happened, or how many individuals were affected.

49. Bluepeak admitted to the Attorney General of Texas that following categories of Private Information were stolen in the Data Breach:

a. Name of individual;

[18] *Id.*

b. Address;

c. Social Security Number Information;

d. Driver's License number;

e. Government-issued ID number (e.g. passport, state ID card);

f. Financial Information (e.g. account number, credit or debit card number);

g. Health Insurance Information; and

h. Date of Birth.[19]

50. Cybercriminals need not harvest a person's Social Security number or financial account information in order to commit identity fraud or misuse Plaintiff's and the Class's Private Information. Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other sources to create "Fullz" packages, which can then be used to commit fraudulent account activity on Plaintiff's and the Class's financial accounts.

The Data Breach was a Foreseeable Risk of Which Defendant was on Notice.

51. It is well known that Private Information, including Social Security numbers, is an invaluable commodity and a frequent target of hackers.

52. Indeed, in 2024, a 3,158 data breaches occurred, exposing approximately 1,350,835,988 sensitive records—a 211% increase year-over-year.[20]

[19] *Data Security Breach Reports*, ATTORNEY GENERAL OF TEXAS, https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage (last visited June 15, 2026).
[20] *2024 Data Breach Annual Report*, IDENTITY THEFT RESOURCE CENTER, https://www.idtheftcenter.org/publication/2024-data-breach-report/ (last visited June 15, 2026).

53. 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. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[21]

54. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgments of data security compromises, and despite its own acknowledgment of its duties to keep Private Information private and secure, Defendant failed to take appropriate steps to protect the Private Information of Plaintiff and Class Members from being compromised.

55. Defendant knew or should have known that Defendant' computer systems were a target for cybersecurity attacks, including ransomware attacks involving data theft, because warnings were readily available and accessible via the internet.

56. In April 2020, ZDNet reported, in an article titled "Ransomware mentioned in 1,000+ SEC filings over the past year," that "[r]ansomware gangs are now ferociously aggressive in their pursuit of big companies. They breach networks, use specialized tools to maximize damage, leak corporate information on dark web portals, and even tip journalists to generate negative news for companies as revenge against those who refuse

[21] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited June 15, 2026).

to pay."[22]

57. In September 2020, the United States Cybersecurity and Infrastructure Security Agency published online a "Ransomware Guide" advising that "[m]alicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion."[23]

58. This readily available and accessible information confirms that, prior to the Data Breach, Defendant knew or should have known that (i) ransomware actors were targeting entities such as Defendant, (ii) ransomware gangs were ferociously aggressive in their pursuit of entities such as Defendant, (iii) ransomware gangs were leaking corporate information on dark web portals, and (iv) ransomware tactics included threatening to release stolen data.

59. Thus, Defendant knew or should have known that they should have encrypted their clients' Social Security numbers and other sensitive data elements to protect against their publication and misuse in the event of a cyberattack.

Plaintiff Todd W Madsen's Experience

60. As a condition of his relationship with Defendant, Plaintiff Madsen was required to supply Defendant with his Private Information.

61. Upon information and belief, Defendant acquired and maintained Plaintiff

[22] Catalin Cimpanu, *Ransomware mentioned in 1,000+ SEC filings over the past year*, ZDNET (Apr. 30, 2020), https://www.zdnet.com/article/ransomware-mentioned-in-1000-sec-filings-over-the-past-year/. (last visited June 15, 2026).
[23] *Ransomware Guide*, U.S. CISA, https://www.cisa.gov/stopransomware/ransomware-guide (last visited June 15, 2026).

Madsen's Private Information as part of its standard business practices and in connection with the services it provides.

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

63. Plaintiff Madsen 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 Madsen 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.

64. Plaintiff Madsen greatly values his privacy and Private Information and takes reasonable steps to maintain the confidentiality of his Private Information. Plaintiff Madsen is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

65. Plaintiff Madsen 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.

66. As a result of the Data Breach, Plaintiff Madsen has spent several hours researching the Data Breach, reviewing his bank accounts, monitoring his credit report, and engaging in other necessary mitigation efforts. This is valuable time that Plaintiff

Madsen would have spent on other activities, including but not limited to work and/or recreation.

67. As a consequence of and following the Data Breach, Plaintiff Madsen has experienced a significant uptick in spam calls, messages, and emails.

68. The Data Breach caused Plaintiff Madsen to suffer stress and anxiety, which were compounded by Defendant's delay in notifying him that his Private Information had been acquired by criminals as a result of the Data Breach.

69. Plaintiff Madsen 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 Madsen will continue to be at present and continued increased risk of identity theft and fraud for years to come.

70. Plaintiff Madsen 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.

71. As a direct and traceable result of the Data Breach, Plaintiff Madsen 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 other sensitive information;

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 Madsen; and

g. other economic and non-economic harm.

Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

72. Plaintiff and members of the proposed Class have suffered injury from the misuse of their Private Information that can be directly traced to Defendant.

73. As a result of Defendant's failure to prevent the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. Plaintiff and the class have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their Private Information is used;

b. The diminution in value of their Private Information;

c. The compromise and continuing publication of their Private Information;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to 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 identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen Private Information; and

h. The continued risk to their Private Information, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the Private Information in its possession.

74. Stolen Private Information is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen Private Information can be worth up to $1,000.00 depending on the type of information obtained.

75. The value of Plaintiff's and the proposed Class's Private Information on the black market is considerable. Stolen Private Information trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

76. Social Security numbers are particularly attractive targets for hackers because they can easily be used to perpetrate identity theft and other highly profitable

types of fraud. Moreover, Social Security numbers are difficult to replace, as victims are unable to obtain a new number until the damage is done.

77. It can take victims years to spot identity or Private Information theft, giving criminals plenty of time to use that information for cash.

78. One such example of criminals using Private Information for profit is the development of "Fullz" packages.

79. Cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

80. The development of "Fullz" packages means that stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiff's and the Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and the Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and members of the Class's stolen Private Information is being misused, and that such misuse is fairly traceable to the Data Breach.

81. Defendant disclosed the Private Information of Plaintiff and members of the

proposed Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the Private Information of Plaintiff and the Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen Private Information.

82. Defendant's failure to properly notify Plaintiff and the Class of the Data Breach exacerbated Plaintiff's and the Class's injuries by depriving them of the earliest ability to take appropriate measures to protect their Private Information and take other necessary steps to mitigate the harm caused by the Data Breach.

Consumers Prioritize Data Security

83. In 2024, the technology and communications conglomerate Cisco published the results of its multi-year "Consumer Privacy Survey."[24] Therein, Cisco reported the following:

a. "For the past six years, Cisco has been tracking consumer trends across the privacy landscape. During this period, privacy has evolved from relative obscurity to a customer requirement with more than 75% of consumer respondents saying they won't purchase from an organization they don't trust with their data."[25]

[24] *Privacy Awareness: Consumers Taking Charge to Protect Personal*, CISCO, https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-consumer-privacy-report-2024.pdf (last visited June 15, 2026).
[25] *Id*. at 3.

b. "Privacy has become a critical element and enabler of customer trust, with 94% of organizations saying their customers would not buy from them if they did not protect data properly."[26]

c. 89% of consumers stated that "I care about data privacy."[27]

d. 83% of consumers declared that "I am willing to spend time and money to protect data" and that "I expect to pay more" for privacy.[28]

e. 51% of consumers revealed that "I have switched companies or providers over their data policies or data-sharing practices."[29]

f. 75% of consumers stated that "I will not purchase from organizations I don't trust with my data."[30]

84. Defendant knew or should have known that adequate implementation of cybersecurity and protection of Private Information, including Plaintiff and the Class's Private Information, was important to its clients.

Defendant failed to adhere to FTC guidelines.

85. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of Private Information.

---

[26] *Id*.
[27] *Id*. at 9.
[28] *Id*.
[29] *Id*.
[30] *Id*. at 11.

86. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

87. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

88. The FTC recommends that companies not maintain 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.

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

obligations.

90. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to clients' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Failed to Follow Industry Standards

91. Several best practices have been identified that—at a minimum—should be implemented by businesses like Defendant. These industry standards include: 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.

92. Other industry standard best practices 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; and training staff regarding critical points.

93. Upon information and belief, Defendant failed to implement industry-standard cybersecurity measures, including failing to meet the minimum standards of both 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).

94. These frameworks are applicable and accepted industry standards. And by

failing to comply with these accepted standards, Defendant opened the door to the criminals—thereby causing the Data Breach.

CLASS ACTION ALLEGATIONS

95. Plaintiff sues on behalf of himself and the proposed nationwide class ("Class, defined as follows, pursuant to Federal Rule of Civil Procedure 23(b)(2) and (b)(3):

> All individuals residing in the United States whose Private Information was compromised in the Data Breach, including all those who received notice of the breach.

96. Excluded from the Class are Defendant, their agents, affiliates, parents, subsidiaries, any entity in which Defendant have a controlling interest, any of Defendant's officers or directors, any successors, and any Judge who adjudicates this case, including their staff and immediate family.

97. Plaintiff reserves the right to amend the class definition.

98. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

a. **Numerosity**. Plaintiff is representative of the Class, consisting of thousands of members, far too many to join in a single action;

b. **Ascertainability**. Members of the Class are readily identifiable from information in Defendant's possession, custody, and control;

c. **Typicality**. Plaintiff's claims are typical of class claims as each arises from the same Data Breach, the same alleged violations by

Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

d. **Adequacy**. Plaintiff will fairly and adequately protect the proposed Class's interests. His interests do not conflict with the Class's interests, and he has retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

e. **Commonality**. Plaintiff's and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for the Class. Indeed, it will be necessary to answer the following questions:

i. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiff's and the Class's Private Information;

ii. 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;

iii. Whether Defendant were negligent in maintaining, protecting, and securing Private Information;

iv. Whether Defendant breached contract promises to safeguard Plaintiff's and the Class's Private Information;

v. Whether Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

vi. Whether Defendant's Data Breach Notice was reasonable;

vii. Whether the Data Breach caused Plaintiff's and the Class's injuries;

viii. What the proper damages measure is; and

ix. Whether Plaintiff and the Class are entitled to damages, treble damages, or injunctive relief.

99. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual plaintiffs are insufficient to make individual lawsuits economically feasible.

FIRST CLAIM FOR RELIEF
Negligence
(On Behalf of Plaintiff and the Class)

100. Plaintiff incorporates all previous paragraphs as if fully set forth herein.

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

102. Defendant owed a duty of care to Plaintiff and Class Members because it was foreseeable that Defendant's failure—to use adequate data security in accordance

with industry standards for data security—would compromise their Private Information in a data breach. And here, that foreseeable danger came to pass.

103. Defendant has full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and the Class could and would suffer if their Private Information was wrongfully disclosed.

104. Defendant owed these duties to Plaintiff and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security practices. After all, Defendant actively sought and obtained Plaintiff and Class Members' Private Information.

105. Defendant owed—to Plaintiff and Class Members—at least the following duties to:

a. exercise reasonable care in handling and using the Private Information in its care and custody;

b. implement industry-standard security procedures sufficient to reasonably protect the information from a data breach, theft, and unauthorized;

c. promptly detect attempts at unauthorized access;

d. notify Plaintiff and Class Members within a reasonable timeframe of any breach to the security of their Private Information.

106. Thus, Defendant owed a duty to timely and accurately disclose to Plaintiff and Class Members the scope, nature, and occurrence of the Data Breach. After all, this

duty is required and necessary for Plaintiff and Class Members to take appropriate measures to protect their Private Information, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

107. Defendant also had a duty to exercise appropriate clearinghouse practices to remove Private Information it was no longer required to retain under applicable regulations.

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

109. Defendant's duty to use reasonable security measures arose because of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential Private Information, a necessary part of obtaining services from Defendant.

110. The risk that unauthorized persons would attempt to gain access to the Private Information and misuse it was foreseeable. Given that Defendant hold vast amounts of Private Information, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the Private Information —whether by malware or otherwise.

111. Private Information is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the Private Information

of Plaintiff and Class Members' and the importance of exercising reasonable care in handling it.

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

113. Defendant breached these duties as evidenced by the Data Breach.

114. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and Class Members' Private Information by:

a. disclosing and providing access to this information to third parties and

b. failing to properly supervise both the way the Private Information was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

115. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and Private Information of Plaintiff and Class Members which actually and proximately caused the Data Breach and Plaintiff and Class Members' injury.

116. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and Class Members, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff and Class Members' injuries-in-fact.

117. Defendant has admitted that the Private Information of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons because of the Data Breach.

118. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and Class Members have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

119. And, on information and belief, Plaintiff's Private Information has already been published—or will be published imminently—by cybercriminals on the Dark Web.

120. Defendant's breach of their common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and Class Members actual, tangible, injury-in-fact and damages, including, without limitation, the theft of f Private Information by criminals, improper disclosure of their Private Information, lost benefit of their bargain, lost value of their Private Information, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

SECOND CLAIM FOR RELIEF
Negligence *Per Se*
(On Behalf of Plaintiff and the Class)

121. Plaintiff incorporates all previous paragraphs as if fully set forth herein.

122. Under the FTC Act, 15 U.S.C. § 45, Defendant had a duty to use fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class

Members' Private Information.

123. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect the Private Information entrusted to it. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff and the Class Members' sensitive Private Information.

124. Defendant breached its respective duties to Plaintiff and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Private Information.

125. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

126. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and members of the Class.

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

128. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that Defendant was failing to meet its duties and that its breach would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their Private Information.

129. Defendant's various violations and its failure to comply with applicable laws and regulations constitute negligence *per se*.

130. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and Class Members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

THIRD CLAIM FOR RELIEF
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

131. Plaintiff incorporates all previous paragraphs as if fully set forth herein.

132. Defendant offered to provide services to or employ Plaintiff and members of the Class if, as a condition of receiving those services or of employment, Plaintiff and members of the Class provided Defendant with their Private Information.

133. In turn, Defendant agreed they would not disclose the Private Information they collects to unauthorized persons. Defendant also promised to safeguard their clients' and Private Information.

134. Plaintiff and the members of the Class accepted Defendant's offers by

providing Private Information to Defendant in exchange for services from Defendant or for employment with Defendant.

135. Implicit in the parties' agreements was that Defendant would provide Plaintiff and members of the Class with prompt and adequate notice of all unauthorized access and/or theft of their Private Information.

136. Plaintiff and the members of the Class would not have entrusted their Private Information to Defendant in the absence of such an agreement with Defendant.

137. Defendant materially breached the contracts they had entered with Plaintiff and members of the Class by failing to safeguard such information and failing to notify them promptly of the intrusion into its computer systems that compromised such information. Defendant also breached the implied contracts with Plaintiff and members of the Class by:

a. Failing to properly safeguard and protect Plaintiff's and members of the Class's Private Information;

b. Failing to comply with industry standards as well as legal obligations that are necessarily incorporated into the parties' agreement; and

c. Failing to ensure the confidentiality and integrity of electronic Private Information that Defendant created, received, maintained, and transmitted.

138. The damages sustained by Plaintiff and members of the Class as described above were the direct and proximate result of Defendant's material breaches of their agreement(s).

139. Plaintiff and members of the Class have performed under the relevant agreements, or such performance was waived by the conduct of Defendant.

140. The covenant of good faith and fair dealing is an element of every contract. All such contracts impose upon each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

141. Subterfuge and evasion violate the obligation of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or may consist of inaction, and fair dealing may require more than honesty.

142. Defendant failed to advise Plaintiff and members of the Class of the Data Breach promptly and sufficiently.

143. In these and other ways, Defendant violated their duty of good faith and fair dealing.

144. Plaintiff and members of the Class have sustained damages because of Defendant's breaches of their agreements, including breaches of it through violations of the covenant of good faith and fair dealing.

145. Plaintiff, on behalf of himself and the Class, seeks compensatory damages for breach of implied contract, which includes the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

FOURTH CLAIM FOR RELIEF
Unjust Enrichment
(On Behalf of the Plaintiff and the Class)

146. Plaintiff incorporates all previous paragraphs as if fully set forth herein.

147. This claim is plead in the alternative to the breach of implied contractual duty claim.

148. Plaintiff and members of the Class conferred a benefit upon Defendant in the form of services through employment. Defendant also benefited from the receipt of Plaintiff's and the Class's Private Information, as this was used to facilitate their employment.

149. Defendant appreciated or had knowledge of the benefits conferred upon itself by Plaintiff and members of the Class.

150. Under principals of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff's and the proposed Class's services and their Private Information because Defendant failed to adequately protect their Private Information. Plaintiff and the proposed Class would not have done business with Defendant, provided their Private Information or worked for Defendant at the payrates they did had they known Defendant would not adequately protect their Private Information.

151. Defendant should be compelled to disgorge into a common fund to benefit Plaintiff and members of the Class all unlawful or inequitable proceeds received by it as a result of the conduct and Data Breach alleged here.

FIFTH CLAIM FOR RELIEF
Breach of Fiduciary Duty
(On Behalf of the Plaintiff and the Class)

152. Plaintiff incorporates all previous paragraphs as if fully set forth herein.

153. Given the relationship between Defendant and Plaintiff and Class members, where Defendant became guardian of Plaintiff's and Class members' Private Information, Defendant became a fiduciary by their undertaking and guardianship of the Private Information, to act primarily for Plaintiff and Class members, (1) for the safeguarding of Plaintiff's and Class members' Private Information; (2) to timely notify Plaintiff and Class members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

154. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class members upon matters within the scope of Defendant's relationship with them—especially to secure their Private Information.

155. Because of the highly sensitive nature of the Private Information, Plaintiff and Class members would not have entrusted Defendant, or anyone in Defendant's position, to retain their Private Information had they known the reality of Defendant's inadequate data security practices.

156. Defendant breached their fiduciary duties to Plaintiff and Class members by failing to sufficiently encrypt or otherwise protect Plaintiff's and Class members' Private Information.

157. Defendant also breached their fiduciary duties to Plaintiff and Class members by failing to diligently discover, investigate, and give notice of the Data Breach

in a reasonable and practicable period.

158. As a direct and proximate result of Defendant's breach of their fiduciary duties, Plaintiff and Class members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

SIXTH CLAIM FOR RELIEF
Declaratory Judgment Act
28 U.S.C. §§ 2201, *Et Seq.*
(On Behalf of Plaintiff and the Class)

159. Plaintiff incorporates all previous paragraphs as if fully set forth herein.

160. This is a claim declaratory relief for Plaintiff and the Class.

161. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. The Court has broad authority to restrain acts, such as those alleged herein, which are tortious and unlawful.

162. Defendant owed a duty of care to Plaintiff and Class Members, which required Defendant to adequately monitor and safeguard Plaintiff's and Class Members' Private Information.

163. Defendant still possesses the Private Information belonging to Plaintiff and Class Members.

164. Plaintiff alleges that Defendant's data security measures remain inadequate. Furthermore, Plaintiff and Class Members continue to suffer injury as a result of the compromise of their Private Information and the risk remains that further compromises of their Private Information will occur in the future.

165. As a result of the Data Breach, an actual controversy has arisen about

Defendant's various duties to use reasonable data security.

166. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owe a legal duty to secure Plaintiff's and Class Members' Private Information under the common law, the FTC Act, and other state and federal laws and regulations, as set forth herein;

b. Defendant's existing data monitoring measures do not comply with its explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices that are appropriate to protect individuals' Private Information; and

c. Defendant continue to breach this legal duty by failing to employ reasonable measures to secure Plaintiff's and Class Members' Private Information.

167. The Court should also issue corresponding injunctive relief requiring Defendant to use adequate security protocols consistent with legal and industry standards to protect the data entrusted to it.

168. If an injunction is not issued, Plaintiff and the Classes will suffer irreparable injury and lack an adequate legal remedy to prevent another data breach of Defendant's computer systems. The risk of another such breach is real, immediate, and substantial. If another breach occurs, Plaintiff and Class Members will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

169. Simply put, monetary damages—while warranted for out-of-pocket

damages and other legally quantifiable and provable damages—cannot cover the full extent of Plaintiff's and Class Members' injuries.

170. The hardship to Plaintiff if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. The cost of Defendant's compliance with an injunction requiring reasonable prospective data security measures is relatively minimal, and Defendant have a pre-existing legal duty to employ such measures.

171. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach of Defendant's systems and network, thus preventing future injury to Plaintiff and to other Class Members whose Private Information would be further compromised.

172. Following the issuance of the declaratory relief requested herein, pursuant to 28 U.S.C. § 2202, Plaintiff and Class Members will seek any further necessary or proper relief, including damages, after reasonable notice and hearing, against Defendant.

PRAYER FOR RELIEF

Plaintiff and members of the Class demand a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing his counsel to represent the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiff

and the Class;

D. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen Private Information;

E. Awarding Plaintiff and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting such other or further relief as may be appropriate under the circumstances.

JURY DEMAND

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

Dated: June 16, 2026

Respectfully Submitted,

/s/ *Melissa M. Meyer*
Melissa M. Meyer
33 Whitehall Street, 27th Floor
New York, NY 10004
Telephone: (212) 363-7500
Facsimile: (212) 363-7171
Email: mmeyer@zlk.com

Raina Borrelli*
STRAUSS BORRELLI PLLC
980 N. Michigan Avenue, Suite 1610
Chicago, Illinois 60611
(872) 263-1100
(872) 263-1109 (facsimile)
sam@straussborrelli.com

* *Pro hac vice forthcoming*

Attorneys for Plaintiff and Proposed Class