

**UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION**

<p>JAMES PRATT, individually and on behalf of all others similarly situated,</p> <p style="text-align: center;">Plaintiff,</p> <p style="text-align: center;">v.</p> <p>FRONTIER COMMUNICATIONS PARENT, INC.,</p> <p style="text-align: center;">Defendant.</p>	<p>Case No. 3:24-cv-01516</p> <p style="text-align: center;"><u>JURY TRIAL DEMANDED</u></p>
---	--

CLASS ACTION COMPLAINT

Plaintiff JAMES PRATT (“Plaintiff”) brings this Class Action Complaint (“Complaint”) against Defendant FRONTIER COMMUNICATIONS PARENT, INC., (“Frontier” or “Defendant”) as an individual and on behalf of all others similarly situated, and alleges, upon personal knowledge as to his own actions and his counsels’ investigation, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. This Class Action arises from a recent cyberattack resulting in a data breach of sensitive information in the possession and custody and/or control of Defendant (the “Data Breach”).

2. The Data Breach resulted in the unauthorized disclosure, exfiltration, and theft of current and former consumers’ highly personal information, including full names, dates of birth, and Social Security numbers, (“personal identifying information” or “PII”).

3. On information and belief, the Data Breach occurred on April 14, 2024. Two months later, on June 6, 2024, Frontier finally notified state Attorneys General and many putative Class Members about the widespread Data Breach (“Notice Letter”). A Sample Notice Letter is attached as **Exhibit A**. Frontier waited two months before informing Class Members about the Data Breach, even though Plaintiff and a staggering 75,895 Class Members had their most sensitive personal information accessed, exfiltrated, and stolen, causing them to suffer ascertainable losses in the form of the loss of the benefit of their bargain and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

4. Frontier’s Breach Notice obfuscated the nature of the breach and the threat it posted—refusing to tell its consumers how many people were impacted, how the breach happened on Frontier’s systems, or why it took Frontier two months to begin notifying victims that hackers had gained access to highly private PII.

5. Defendant’s failure to timely detect and report the Data Breach made its consumers vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their PII.

6. Defendant knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of PII misuse.

7. In failing to adequately protect Plaintiff’s and the Class’s PII, failing to adequately notify them about the breach, and by obfuscating the nature of the breach, Defendant violated state and federal law and harmed tens of thousands of its current and former consumers.

8. Plaintiff and members of the proposed Class are victims of Defendant’s negligence and inadequate cyber security measures. Specifically, Plaintiff and members of the proposed Class

trusted Defendant with their PII. But Defendant betrayed that trust. Defendant failed to properly use up-to-date security practices to prevent the Data Breach.

9. Plaintiff is a Data Breach victim.

10. Accordingly, Plaintiff, on his own behalf and on behalf of a class of similarly situated individuals, brings this lawsuit seeking injunctive relief, damages, and restitution, together with costs and reasonable attorneys' fees, the calculation of which will be based on information in Defendant's possession.

PARTIES

11. Plaintiff, James Pratt, is a natural person and citizen of Illinois, where he intends to remain.

12. Defendant, Frontier Communications Parent Inc., is a Delaware incorporated company, with its principal place of business at 211 E 7th Street Suite 620 Austin, Texas 78701-3218. Defendant can be served through its registered agent, Corporation Service Company D/B/A CSC-Lawyers Inco. at 211 E 7th Street Suite 620 Austin, Texas 78701-3218.

JURISDICTION AND VENUE

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

14. This Court has personal jurisdiction over Defendant because Defendant maintains its principal place of business in the Dallas Division of the Northern District of Texas and does substantial business in this District.

15. Venue is proper in Dallas Division of the Northern District of Texas under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claim occurred in this District.

STATEMENT OF FACTS

Frontier

16. Frontier is a telecommunication company that touts itself as the “largest pure-play fiber provider in the United States” that “deliver[s] blazing-fast broadband connectivity that unlocks the potential of millions of consumers and business.”¹ Frontier boasts a total annual revenue of over \$1.3 billion.²

17. On information and belief, Frontier accumulates highly private PII of its current and former consumers.

18. In collecting and maintaining its consumers’ PII, Defendant agreed it would safeguard the data in accordance with state law and federal law. After all, Plaintiff and Class Members themselves took reasonable steps to secure their PII.

19. As a self-proclaimed leader in its industry, Frontier understood the need to protect its consumers’ data and prioritize its data security.

20. Indeed, Fronter promises in its Privacy Policy to “use reasonable technical, administrative, and physical safeguards to protect against unauthorized access to, use of, or disclosure of the personal information we collect and store.”³

¹ Frontier, LinkedIn, <https://www.linkedin.com/company/frontier-communications/> (last visited June 14, 2024).

² Frontier, Zoominfo <https://www.zoominfo.com/c/frontier-communications-corp/20317318> (last visited June 14, 2024).

³ Privacy Policy, Frontier, <https://frontier.com/corporate/privacy-policy> (last visited June 14, 2024).

21. Despite recognizing its duty to do so, on information and belief, Frontier has not implemented reasonably cybersecurity safeguards or policies to protect its consumers' PII or supervised its IT or data security agents and employees to prevent, detect, and stop breaches of its systems. As a result, Frontier leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to consumers' PII.

The Data Breach

22. Plaintiff is a Frontier consumer. As a condition of receiving Frontier's telecommunication services, Plaintiff provided Frontier with his PII. Frontier used that PII to facilitate its services of Plaintiff and required Plaintiff to provide that PII to obtain services.

23. On information and belief, Defendant collects and maintains consumers' PII in its computer systems.

24. According to the Breach Notice, on April 14, 2024, Frontier discovered "unauthorized access to some of [its] internal IT systems." Ex. A. Following an internal investigation, Frontier discovered that a Data Breach had occurred and that, as a result, "your personal information among the data affected." Ex. A.

25. In other words, Frontier's investigation revealed that its cyber and data security systems were completely inadequate and allowed cybercriminals to obtain files containing a treasure trove of thousands of its consumers' highly private PII.

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

27. On information and belief, the notorious Ransomhub ransomware gang claimed responsibility for the cyberattack on June 4, 2024. Since coming onto the scene in February of this year, Ransomhub has become one of the most active ransomware actors and the center of numerous

large scale data breaches.⁴ Frontier, a self-proclaimed leader in its industry, knew or should have known of the tactics that groups like Ransomhub employ.

RansomHub

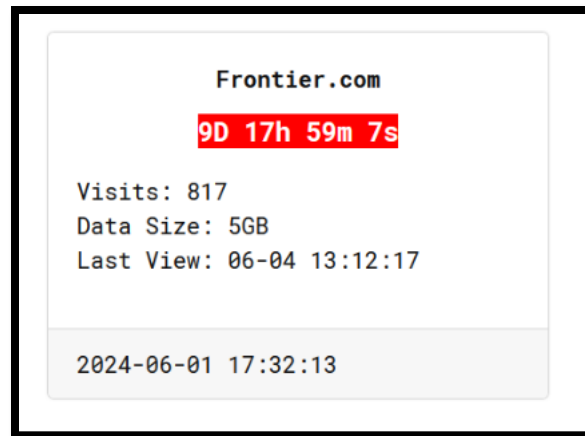
Frontier.com

Data is more than 2 million customer with address name email ssn credit score date of birth and phone number. We gave frontier 2 months to contact us but they don't care about clients data. Below is screenshot of some of the data.

Now anyone who wants to buy this data can contact our blog support, we only sell it once



⁴ The Register, What is RansomHub, https://www.theregister.com/2024/06/05/ransomhub_knight_reboot/ (June 14, 2024)



28. With the PII secured and stolen by Ransomhub, the hackers then purportedly issued a ransom demand to Frontier. However, Frontier has provided no public information on the ransom demand or payment.

29. On information and belief, Ransomhub is anticipated to release all 5GB of stolen data onto the dark web on June 14, 2024, the presumed deadline of Ransomhub's ransom demand,

30. On or around March 18, 2024 –two months after the Breach first occurred and only after Ransomhub publicly announced its role perpetrating the Data Breach and holding Plaintiff and the Class's PII ransom – Frontier finally notified Plaintiff and Class Members about the Data Breach.

31. Despite its duties and alleged commitments to safeguard PII, Defendant did not in fact follow industry standard practices in securing consumers' PII, as evidenced by the Data Breach.

32. In response to the Data Breach, Defendant contends that it has taken "steps to further strengthen [its] network security[.]" Ex. A. Although Defendant fails to expand on what these alleged "steps" are, such security measures should have been in place before the Data Breach.

33. Through the Data Breach, Defendant recognized its duty to implement reasonable cybersecurity safeguards or policies to protect consumers' PII, insisting that, despite the Data Breach demonstrating otherwise, Defendant "take[s] seriously the security of your data" and "take[s] seriously the responsibility to protect the information entrusted to us and regret any inconvenience this incident may have caused you." Ex. A.

34. Through its Breach Notice, Defendant also recognized the actual imminent harm and injury that flowed from the Data Breach, so it encouraged breach victims to "remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors." Ex. A.

35. 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 PII. 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.

36. On information and belief, Frontier has offered several months of complimentary credit monitoring services to victims, which does not adequately address the lifelong harm that victims will face following the Data Breach. Indeed, the breach involves PII that cannot be changed, such as Social Security numbers.

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

38. Because of the Data Breach, Defendant inflicted injuries upon Plaintiff and Class Members. And yet, Defendant has done absolutely nothing to provide Plaintiff and the Class Members with relief for the damages they suffered and will suffer.

39. On information and belief, Defendant failed to adequately train and supervise its IT and data security agents and employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over its consumers' PII. Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the PII.

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

40. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the telecommunications industry preceding the date of the breach.

41. In light of recent high profile data breaches at other communication provider and partner companies, Defendant knew or should have known that its electronic records and consumers' PII would be targeted by cybercriminals.

42. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.⁵ The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.⁶

⁵ 2021 Data Breach Annual Report, ITRC, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.wsav.com/wp-content/uploads/sites/75/2022/01/20220124_ITRC-2021-Data-Breach-Report.pdf (last visited June 5, 2023).

⁶ *Id.*

43. Indeed, cyberattacks against the telecommunications industry have become increasingly common for over ten years, with the FBI warning as early as 2011 that cybercriminals were “advancing their abilities to attack a system remotely” and “[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII.” The FBI further warned that that “the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime.”⁷

44. Cyberattacks on companies like Defendant 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 prepared for, a potential attack. As one report explained, “[e]ntities like smaller municipalities and hospitals are attractive. . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly.”⁸

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

Plaintiff’s Experience

46. Plaintiff received Frontier’s Breach Notice on or around June 2024.

47. Defendant deprived Plaintiff of the earliest opportunity to guard himself against the Data Breach’s effects by failing to notify him about it for two months.

48. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff’s PII for theft by cybercriminals, including Ransomhub, and sale on the dark web.

⁷ Gordon M. Snow Statement, FBI <https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector> (last visited March 13, 2023).

⁸ Secret Service Warn of Targeted, Law360, <https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware> (last visited March 13, 2023).

49. As a result of the Data Breach notice, Plaintiff spent uncompensated time dealing with the consequences of the Data Breach, which includes uncompensated time spent verifying the legitimacy of the Notice of Data Breach, self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This uncompensated time has been lost forever and cannot be recaptured.

50. Plaintiff has and will spend considerable time and effort monitoring his accounts to protect himself from additional identity theft. Plaintiff fears for his personal financial security and uncertainty over what PII was exposed in the Data Breach.

51. Plaintiff has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

52. Plaintiff suffered actual injury in the form of damages to and diminution in the value of Plaintiff's PII—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

53. Plaintiff suffered actual injury from the exposure and theft of his PII—which violates his rights to privacy.

54. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of unauthorized third parties and possibly criminals.

55. Indeed, shortly after the Data Breach, Plaintiff was notified by Capital One that his home address and phone number was recently detected on the dark web, suggesting that his PII is now in the hands of cybercriminals.

56. Further, following the Data Breach, Plaintiff began receiving a significant amount of spam calls and texts regarding loans and national debt relief program, further suggesting that his PII is now in the hands of cybercriminals.

57. Once an individual's PII is for sale and access on the dark web, as Plaintiff's PII is here as a result of the Breach, cybercriminals are able to use the stolen and compromised to gather and steal even more information.⁹ On information and belief, Plaintiff's phone number was compromised as a result of the Data Breach.

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

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

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

60. 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. They have suffered or are at an increased risk of suffering:

- a. The loss of the opportunity to control how their PII is used;
- b. The diminution in value of their PII;
- c. The compromise and continuing publication of their PII;

⁹ What do Hackers do with Stolen Information, Aura, <https://www.aura.com/learn/what-do-hackers-do-with-stolen-information> (last visited January 9, 2024).

- 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 PII; and
- h. The continued risk to their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the PII in its possession.

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

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

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

64. One such example of criminals using PII for profit is the development of "Fullz" packages.

65. Cyber-criminals can cross-reference two sources of PII 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.

66. The development of “Fullz” packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff and the proposed Class’ 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 PII 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 members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff’s and the Class’s stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

67. Defendant disclosed the PII of Plaintiff and the Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII 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 PII.

68. Defendant’s failure to properly notify Plaintiff and members of the Class of the Data Breach exacerbated Plaintiff’s and the Class’s injury by depriving them of the earliest

ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

Defendant failed to adhere to FTC guidelines.

69. 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 PII.

70. 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 sensitive consumer information that it keeps;
- b. properly dispose of PII 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.

71. 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.

72. 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.

73. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer 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.

74. Defendant’s failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers’ PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Fails to Comply with Industry Standards

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

76. Several best practices have been identified that a minimum should be implemented by employers in possession of PII, 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.

77. Other best cybersecurity practices that are standard for employers 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.

78. Upon information and belief Defendant failed to meet the minimum standards of one or more of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

79. These foregoing frameworks are existing and applicable industry standards for an employer's obligations to provide adequate data security for its employees. 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.

CLASS ACTION ALLEGATIONS

80. Plaintiff brings this class action under Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), individually and on behalf of all members of the following class:

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

81. Excluded from the Class is 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.

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

83. 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 at least 751,895 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 PII;
 - 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 PII;

- iv. Whether Defendant breached contract promises to safeguard Plaintiff's and the Class's PII;
- v. Whether Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;
- vi. Whether Defendant's 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.

84. 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.

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

85. Plaintiff realleges all previous paragraphs as if fully set forth below.

86. Plaintiff and members of the Class entrusted their PII to Defendant. Defendant owed to Plaintiff and the Class a duty to exercise reasonable care in handling and using the PII in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

87. Defendant owed a duty of care to Plaintiff and members of the Class because it was foreseeable that Defendant's failure to adequately safeguard their PII in accordance with

state-of-the-art industry standards concerning data security would result in the compromise of that PII —just like the Data Breach that ultimately came to pass. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff’s and the Class’s PII by disclosing and providing access to this information to unauthorized third parties and by failing to properly supervise both the way the PII was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

88. Defendant owed to Plaintiff and members of the Class a duty to notify them within a reasonable timeframe of any breach to the security of their PII. Defendant also owed a duty to timely and accurately disclose to Plaintiff and members of the Class the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiff and the Class to take appropriate measures to protect their PII, 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.

89. Defendant owed these duties to Plaintiff and members of the Class 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 protocols. Defendant actively sought and obtained Plaintiff’s and the Class’s PII.

90. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Defendant holds vast amounts of PII, it was inevitable that unauthorized individuals would attempt to access Defendant’s databases containing the PII —whether by malware or otherwise.

91. PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiff and the Class and the importance of exercising reasonable care in handling it.

92. Defendant breached its duties by failing to exercise reasonable care in supervising its employees, agents, contractors, vendors, and suppliers, and in handling and securing the PII of Plaintiff and the Class which actually and proximately caused the Data Breach and Plaintiff's and the Class's injury. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and members of the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff's and members of the Class's injuries-in-fact. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and the Class have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

93. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and members of the Class actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, 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.

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiff and the Class)

94. Plaintiff realleges all previous paragraphs as if fully set forth below.

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

96. 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 customers or, in this case, consumers’ PII. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant’s duty to protect Plaintiff’s and the members of the Class’s PII.

97. Defendant breached its 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 PII.

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

99. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiff’s and the Class’s PII and not complying with applicable industry standards as described in detail herein. Defendant’s conduct was particularly unreasonable given the nature and amount of PII Defendant 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.

100. 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 the Class.

101. But for Defendant's wrongful and negligent breach of the duties owed to Plaintiff and members of the Class, Plaintiff and members of the Class would not have been injured.

102. The injury and harm suffered by Plaintiff and members of the Class were the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it 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 PII.

103. Had Plaintiff and the Class known that Defendant did not adequately protect their PII, Plaintiff and members of the Class would not have entrusted Defendant with their PII.

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

105. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of PII; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen PII, entitling them to damages in an amount to be proven at trial.

106. Additionally, as a direct and proximate result of Defendant's negligence *per se*, Plaintiff and Class members have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized

disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect their PII in its continued possession.

COUNT III
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

107. Plaintiff realleges all previous paragraphs as if fully set forth below.

108. Plaintiff and Class members were required to provide their PII to Defendant as a condition of receiving services provided by Defendant. Plaintiff and Class members provided their PII to Defendant or its third-party agents in exchange for Defendant's communication services.

109. Plaintiff and Class members reasonably understood that a portion of the funds they paid Defendant would be used to pay for adequate cybersecurity measures.

110. Plaintiff and Class members reasonably understood that Defendant would use adequate cybersecurity measures to protect the PII that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

111. Plaintiff and the Class members accepted Defendant's offers by disclosing their PII to Defendant or its third-party agents in exchange for telecommunication services.

112. In turn, and through internal policies, Defendant agreed to protect and not disclose the PII to unauthorized persons.

113. In its Privacy Policy, Defendant represented that they had a legal duty to protect Plaintiff's and Class Member's PII.

114. Implicit in the parties' agreement was that Defendant would provide Plaintiff and Class members with prompt and adequate notice of all unauthorized access and/or theft of their PII.

115. After all, Plaintiff and Class members would not have entrusted their PII to Defendant or its third-party agents in the absence of such an agreement with Defendant.

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

117. The covenant of good faith and fair dealing is an element of every contract. Thus, 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—and not merely the letter—of the bargain. In short, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

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

119. Defendant materially breached the contracts it entered with Plaintiff and Class members by:

- a. failing to safeguard their information;
- b. failing to notify them promptly of the intrusion into its computer systems that compromised such information.
- c. failing to comply with industry standards;
- d. failing to comply with the legal obligations necessarily incorporated into the agreements; and
- e. failing to ensure the confidentiality and integrity of the electronic PII that Defendant created, received, maintained, and transmitted.

120. In these and other ways, Defendant violated its duty of good faith and fair dealing.

121. Defendant's material breaches were the direct and proximate cause of Plaintiff and Class members' injuries (as detailed *supra*).

122. Plaintiff and Class members performed as required under the relevant agreements, or such performance was waived by Defendant's conduct.

COUNT IV
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

123. Plaintiff realleges all previous paragraphs as if fully set forth below.

124. Plaintiff and members of the Class conferred a benefit upon Defendant in providing PII to Defendant.

125. Defendant appreciated or had knowledge of the benefits conferred upon it by Plaintiff and the Class. Defendant also benefited from the receipt of Plaintiff's and the Class's PII, as this was used to facilitate its services to Plaintiff and the Class.

126. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII.

127. Instead of providing a reasonable level of security, or retention policies, which would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

128. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff's and the Class's PII because Defendant failed to adequately protect their PII.

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

130. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and members of the Class all unlawful or inequitable proceeds received by them because of their misconduct and Data Breach.

COUNT V
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Class)

131. Plaintiff realleges all previous paragraphs as if fully set forth below.

132. Given the relationship between Defendant and Plaintiff and Class Members, where Defendant became guardian of Plaintiff's and Class Members' PII, Defendant became a fiduciary by its undertaking and guardianship of the PII, to act primarily for Plaintiff and Class Members, (1) for the safeguarding of Plaintiff's and Class Members' PII; (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.

133. 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 PII.

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

135. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to sufficiently encrypt or otherwise protect Plaintiff's and Class Members' PII.

136. Defendant also breached its 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.

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

COUNT VI
Intrusion upon Seclusion/Invasion of Privacy
(On Behalf of Plaintiff and the Class)

138. Plaintiff realleges all previous paragraphs as if fully set forth below.

139. The State of Texas recognizes the tort of Intrusion upon Seclusion, and adopts the formulation of that tort found in the Restatement (Second) of Torts, which states:

One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.

Restatement (Second) of Torts § 652B (1977).

140. Plaintiff and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential PII and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

141. Defendant owed a duty to its current and former consumers, including Plaintiff and the Class, to keep this information confidential.

142. The unauthorized acquisition (i.e., theft) by a third party of Plaintiff's and Class members' PII is highly offensive to a reasonable person.

143. The intrusion was into a place or thing which was private and entitled to be private. Plaintiff and the Class disclosed their sensitive and confidential information to Defendant, but did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiff and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

144. The Data Breach constitutes an intentional interference with Plaintiff's and the Class's interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

145. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

146. Defendant acted with a knowing state of mind when it failed to notify Plaintiff and the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

147. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and the Class.

148. As a proximate result of Defendant's acts and omissions, the private and sensitive PII of Plaintiff and the Class were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages (as detailed *supra*).

149. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their PII are still maintained by Defendant with their inadequate cybersecurity system and policies.

150. Plaintiff and the Class have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the PII of Plaintiff and the Class.

151. In addition to injunctive relief, Plaintiff, on behalf of himself and the other Class members, also seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest and costs.

PRAYER FOR RELIEF

Plaintiff and 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 representatives, and appointing their 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 PII;
- 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 TRIAL DEMANDED

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

Dated: June 18, 2024,

Respectfully submitted,

By: /s/ Joe Kendall

JOE KENDALL
Texas Bar No. 11260700
KENDALL LAW GROUP, PLLC
3811 Turtle Creek Blvd., Suite 825
Dallas, Texas 75219
214-744-3000 / 214-744-3015 (Facsimile)
jkendall@kendalllawgroup.com

STRAUSS BORRELLI PLLC
Samuel J. Strauss (*Pro Hac Vice* forthcoming)
Raina C. Borrelli (*Pro Hac Vice* forthcoming)

980 N. Michigan Avenue, Suite 1610
Chicago, Illinois 60611
(872) 263-1100
(872) 263-1109 (facsimile)
sam@straussborrelli.com
raina@straussborrelli.com

Attorneys for Plaintiff and Proposed Class