UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

PATRICK MAYS, on behalf of himself and all others similarly situated, Plaintiff, v. **FRONTIER COMMUNICATIONS PARENT, INC.** Defendant.	No.3:24-cv-01468 **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Patrick Mays, individually and on behalf of all others similarly situated, files this Class Action Complaint against Frontier Communications Parent, Inc. and alleges the following based on personal knowledge of facts pertaining to him and the investigation of counsel as to all other matters:

NATURE OF THE ACTION

1. Frontier Communications Parent, Inc. ("Frontier") is an American telecommunications company servicing residential and business customers in 25 states. As of 2021, Frontier had around 3 million broadband subscribers and a fiber optic network including 5.2 million locations. This class action arises out of a recent cyberattack and data breach ("Data Breach") that resulted in the theft and exfiltration of hundreds of thousands of Frontier customers' personally identifying information, including, at a minimum, full names, social security numbers, physical addresses, dates of birth, email addresses, credit scores, and phone numbers ("PII").

2. As part of its business model, Frontier collects consumers' PII along with drivers' license numbers and payment information. Frontier retains this personal information not just to facilitate delivery of telecommunications services, but for its own business interests and profits—including selling and sharing personal information through the use of cookies and trackers.

3. Frontier promises to "protect[]" its customers' privacy and to use "reasonable technical, administrative, and physical safeguards to protect against unauthorized access to, use of, or disclosure of consumers' PII."[1]

4. Frontier also promises to limit the third parties to whom it makes customers' PII available, committing to share personal information only with "third party agents and vendors that perform services on our behalf," which Frontier supposedly "requires" to "use . . . only as we direct, and to protect [the information] consistent with this policy." Other than the limited uses laid out in its Privacy Policy, Frontier promises that "**We do not otherwise share your personal information**."

5. But in April 2024, Frontier failed to protect the information of over 751,000 Frontier customers who entrusted it with their PII. Threat actors breached Frontier's computer systems and data, stole 5GB of customer data, and has threatened to post the data on the internet unless Frontier pays a ransom by June 14, 2024. The thieves claim that the stolen dataset contains full names, social security numbers, physical addresses, dates of birth, email addresses, credit scores, and phone numbers.[2]

---

[1] Frontier, *Privacy Policy* https://frontier.com/corporate/privacy-policy (last visited June 10, 2024). For California customers, Frontier maintains a separate California Privacy Policy, available at https://frontier.com/corporate/privacy-policy-california.

[2] Jess Weatherbed, *Frontier hackers threaten to release private data for at least 750,000 customers*, The Verge (June 10, 2024), https://www.theverge.com/2024/6/10/24175169/frontier-

6. In a filing with the U.S. Securities and Exchange Commission ("SEC"), Frontier acknowledged the attack and admitted that it had to shut down certain company systems in order to contain it. Frontier reported to the SEC that "the third party was likely a cybercrime group, which gained access to, among other information, personally identifiable information."

7. Plaintiff is a loyal Frontier customer who trusted Frontier with personal information while purchasing telecommunications services. Now, Plaintiff brings this class action to hold Frontier accountable for its failure to adequately secure and protect its customers' PII.

8. By collecting and retaining Plaintiff's and the Class Members' PII for its own financial benefit, Frontier assumed a duty to Plaintiff and the Class Members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII against unauthorized access and disclosure. Frontier also had a duty to safeguard this PII under applicable case law, industry standards, and statutory obligations, including Section 5 of the Federal Trade Commission Act ("FTC Act").

9. But Frontier breached those duties by, among other things, failing to implement and maintain reasonable security procedures and practices to protect the PII in its possession. The Data Breach was directly traceable to Frontier's failure to implement proper security protocols and, among other things, neglecting to implement adequate and reasonable measures to secure consumers' data systems against unauthorized intrusions; withholding disclosure regarding insufficiently robust computer systems and security practices to safeguard PII; omitting standard and reasonably available steps to prevent the Data Breach; inadequately training its staff and employees on proper security measures; and failing to promptly and

communications-hack-cyberattack-data-breach-ransom.

adequately notify Plaintiffs and the Class Members of the Data Breach. Frontier also neglected proper monitoring of its network, which could have detected the intrusion before the thieves exfiltrated the PII or potentially prevented the intrusion altogether.

10. Because of Frontier's acts and omissions, Plaintiff's and the Class Members' PII is now in the hands of, in Frontier's words, "a cybercrime group." Now, Plaintiff and the Class Members must diligently monitor their financial accounts to thwart potential identity theft. They will need to bear out-of-pocket expenses for and spend uncompensated time on credit monitoring, obtaining identity theft protection, retrieving and reviewing credit reports, and taking other protective measures—both now and in the future. Plaintiff and the Class Members have suffered diminished value to their bargain with Frontier, out-of-pocket expenses associated with protecting their privacy and security, and the value of their time spent addressing or mitigating the effects of the attack.

11. Moreover, Frontier still maintains Plaintiff's and the Class Members' PII. Without additional safeguards and independent review, this information remains susceptible to further cyberattacks and theft.

12. Plaintiff and members of the Class have suffered irreparable harm, including the exposure of their PII to nefarious strangers and their significantly increased risk of identity theft. The information at issue here is the very kind of information that allows identity thieves to construct false identities and invade all aspects of Plaintiff's and the Class Members' lives. In addition to facing the emotional devastation of having such personal information fall into the wrong hands, Plaintiff and the Class members must now undertake additional security measures and precautions to minimize their risk of identity theft. And the ongoing risk to Plaintiff and the Class Members will persist throughout their lifetimes.

PARTIES

13. Plaintiff Patrick Mays is and at all relevant times has been a citizen of Richwood, West Virginia.

14. Plaintiff has an account with Frontier. Plaintiff provided his PII to Frontier in connection with his Frontier account.

15. Plaintiff received a notice from Frontier stating that his PII had been stolen in a cyberattack. A copy of the notice is attached as **ATTACHMENT A.**

16. Plaintiff is deeply concerned about the Data Breach, as his PII is now readily available for cybercriminals to sell, buy, or exchange on the Dark Web.

17. Plaintiff has a continuing interest in ensuring that his PII, which remains in Frontier's possession, is protected and safeguarded from future breaches.

18. Defendant Frontier is a Delaware corporation with a principal place of business located at 1919 McKinney Avenue, Dallas, Texas 75201. The registered agent for service of process is Corporation Service Company d/b/a CSC – Lawyers Incorporating Service Company, 211 E. 7th Street, Suite 620, Austin, Texas 78701-3218.

JURISDICTION AND VENUE

19. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. At least one member of the Class, defined below, is a citizen of a different state than Frontier, including Plaintiff, and there are more than 100 putative Class members. Plaintiff is a citizen of West Virginia. Defendant is a citizen of Texas.

20. This Court has personal jurisdiction over Frontier because its principal place of business is in the Dallas Division of the Northern district of Texas and it regularly transacts

business in this District.

21. Venue is proper in this District under 28 U.S.C. § 1391(a)(1) because Frontier's principal place of business is located in the Dallas Division of the Northern District of Texas and a substantial part of the events giving rise to this action occurred in this District.

FACTUAL ALLEGATIONS

A. Frontier chooses to collect and keep consumers' PII.

22. Frontier provides services including broadband internet, a fiber-optic network, cloud-based services, digital television, and computer technical support to millions of Americans across 25 states.

23. Originally incorporated in 1935, the company began focusing solely on telecommunications in the late 1990s. Subsequently, Frontier acquired assets from telecommunications companies like Verizon Communications and AT&T, growing its operations to include service in multiple large states. After filing for bankruptcy and emerging from restructuring, Frontier went public on the NASDAQ in 2021. Frontier reported revenues over $5.75 billion in 2023.[3]

24. Frontier requires customers to provide it with their PII, both to facilitate delivery of telecommunications services and for its own business purposes. In return, Frontier promises to keep consumers' PII secure and that it will not sure consumers' private information with unauthorized third parties.

25. Frontier maintains the "Frontier Communications Privacy Policy," which states

[3] GuruFocus Research, *Frontier Communications Parent Inc. Reports EBITDA Growth Amid Fiber Expansion*, Yahoo!Finance (Feb. 23, 2024), https://finance.yahoo.com/news/frontier-communications-parent-inc-fybr-125311963.html.

that "Protecting the privacy of our customers is important to Frontier."[4] The Privacy Policy also states that Frontier will use reasonable technical, administrative, and physical safeguards to protect against unauthorized access to, use of, or disclosure of the personal information that Frontier collects and stores. Frontier also promises to retain records only as long as reasonably necessary for business, accounting, or tax purposes.

26. The Privacy Policy identifies the information that Frontier collects from consumers, including name, contact information, driver's license number, Social Security number, payment information, research records, call records, records of website visits, information about devices used in connection with Frontier's services, bandwidth usage, TV and video viewership, IP address and device identification numbers, and information from devices on which the Frontier Android App is installed.

27. The Privacy Policy also contains promises about how Frontier will use the information it collects. Specifically, the Privacy Policy promises that Frontier will *only* share consumers' personal information, including PII, with specified third parties. Apart from the uses laid out in the Privacy Policy, Frontier promises that "We do not otherwise share your personal information."

28. Plaintiff and the Class Members entrusted their PII to Frontier with the reasonable expectation and mutual understanding that Frontier would fulfill its obligations to maintain the confidentiality and security of their information, safeguarding it against unauthorized access.

B. Frontier failed to protect consumers' private information.

29. Despite Frontier's explicit assurances that it would employ reasonable measures

[4] Frontier, *Privacy Policy* https://frontier.com/corporate/privacy-policy (last visited June 10, 2024).

to safeguard consumers' PII, and only share that information with expressly authorized individuals, Frontier allowed a cybercrime group to infiltrate its systems and steal PII belonging to over 751,000 of its customers.

30. On April 14, 2024, Frontier detected unauthorized access to some of its internal IT systems. Although Frontier shut down some of its systems, creating an operational disruption, it failed to prevent the threat actor from exfiltrating consumers' personal information, including, reportedly, full names, physical addresses, dates of birth, social security numbers, email addresses, credit scores, and phone numbers. Many customers reported that their internet connection went down during the attack, with support phone numbers playing a prerecorded message instead of redirecting to a human operator.[5]

31. In a regulatory filing with the SEC, Frontier stated that "it has determined that the third party was likely a cybercrime group which gained access to, among other information, personally identifiable information."

32. The "cybercrime group" in question is reportedly RansomHub, a notorious extortion group. On June 4, 2024, RansomHub added Frontier Communications to its "extortion portal" on the Dark Web, threatening to leak 5 GB of stolen data unless Frontier agreed to pay a hefty ransom.[6] Although Frontier's official statements regarding the breach indicate that just over 751,000 consumers were affected, RansomHub has boasted that the stolen data includes information belonging to two million customers.

33. RansomHub has claimed credit for several recent data breaches, including a

[5] Bill Toulas, *Frontier warns 750,000 of a data breach after extortion threats*, Bleeping Computer (June 7, 2024), https://www.bleepingcomputer.com/news/security/frontier-warns-750-000-of-a-data-breach-after-extortion-threats.
[6] *Id.*

cyberattack targeting the British auction house Christie's[7] and the theft of highly sensitive personal health information from Change Healthcare.[8]

34. Frontier unreasonably waited almost two months to begin notifying consumers of the breach. Although Frontier became aware of the breach on April 14, 2024, it waited until June 6, 2024 to begin notifying consumers who were affected. Time is crucial when highly sensitive PII is subjected to unauthorized access and/or acquisition. The disclosed, accessed, and/or acquired PII of the Plaintiff and the Class Members may now be available on the Dark Web, for sale to criminals. As a result, the Plaintiff and the Class Members are currently and continuously exposed to the risk of fraud, identity theft, and misuse stemming from the potential publication of their PII.

35. Frontier's belated notice also lacks sufficient details to put consumers on notice of the threats to their privacy. Frontier's notice admits that there was "unauthorized access to some of our internal IT systems" and states that "personal information was among the data affected." Plaintiff and the Class Members remain in the dark about the extent of the data breach; the specific data stolen; and the measures, if any, being implemented to safeguard their PII moving forward. Indeed, Frontier's notice did not identify the threat actor—or even that the data was stolen. Plaintiff and the Class Members are left to speculate about the complete ramifications of the Data Breach and the precise strategies Frontier plans to employ to enhance its information security systems and monitoring capabilities in order to avert future breaches

36. Frontier has also done next to nothing to repair the damage its negligence caused.

---

[7] Alexander Martin, *RansomHub claims attack on Christie's, the world's wealthiest auction house*, The Record (May 28, 2024), https://therecord.media/christies-cyberattack-ransomhub-claims.

[8] Eric Geller, *Change Healthcare's New Ransomware Nightmare Goes from Bad to Worse*, Wired (April 16, 2024), https://www.wired.com/story/change-healthcare-ransomhub-data-sale/.

Frontier stated that it would provide only a year of credit monitoring services—a woefully inadequate offer since the risks of identity theft persist well beyond one year and can last a lifetime. Frontier has offered no additional safeguards to shield Plaintiff and the Class Members from the enduring threats now facing them.

37. Instead, Frontier purports to put the burden of identity protection on Plaintiff and the Class Members by advising them 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." Frontier does not offer to compensate Plaintiff or the Class Members for time spent on such activities, although Frontier's own acts and omissions led to the need for such precautions.

C. The Data Breach is directly traceable to Frontier's acts and omissions, including its negligence and the breach of its duties to Plaintiff and the Class.

38. Frontier is responsible for allowing the Data Breach to occur because it failed to implement and maintain reasonable safeguards, failed to comply with industry-standard data security practices, as well as federal and state laws and regulations governing data security, and failed to supervise, monitor, and oversee all third parties it hired who had access to Plaintiff's and the Class members' PII.

39. During the Data Breach, Frontier failed to adequately monitor its information technology infrastructure. Had Frontier done so, it would have prevented or mitigated the scope and impact of the Data Breach.

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

41. Plaintiff's and the Class Members' PII was provided to Frontier with the reasonable expectation and understanding that Frontier would comply with its obligations to keep such information confidential and secure from unauthorized access.

42. Cyberattacks have become so prevalent that the FBI and U.S. Secret Service have issued warnings to potential targets, urging them to be aware of and prepared for potential attacks.[9]

43. Frontier's data security obligations were particularly important given the substantial increase in cyber and ransomware attacks and data breaches in the financial services industries preceding the date of the Data Breach, as well as given the incredibly sensitive nature of PII that it retained in its servers.

D. Frontier failed to comply with FTC guidelines.

44. The FTC Act, 15 U.S.C. § 45, prohibits Frontier from committing "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has determined that a company's failure to uphold reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

45. The FTC has issued guidelines for businesses emphasizing the significance of adopting reasonable data security practices. According to the FTC, integrating data security considerations into all aspects of business decision-making is imperative. A

46. In 2016, the FTC issued an updated version of its publication, "Protecting Personal Information: A Guide for Business," which established cyber-security guidelines for businesses.[10]

[9] Ben Kochman, FBI, Secret Service Warn of Targeted Ransomware, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974.

[10] Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-

These guidelines underscored the importance for businesses to safeguard personal customer information, securely dispose of unnecessary personal data, encrypt information stored on computer networks, assess network vulnerabilities, and institute policies to address security issues promptly. Additionally, the guidelines recommend using intrusion detection systems to promptly detect breaches, monitoring incoming traffic for signs of hacking attempts, being vigilant about large data transmissions, and having a response plan prepared in the event of a breach.[11]

47. The FTC also advises that companies not retain PII longer than necessary for transaction authorization, restrict access to sensitive data, enforce the use of complex passwords on networks, employ industry-tested security methods, monitor the network for suspicious activity, and ensure that third-party service providers have implemented adequate security measures.

48. The FTC has brought enforcement actions against businesses for failing to protect customer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice.

49. Frontier failed to properly implement basic data security practices by failing to employ reasonable and appropriate measures to protect against unauthorized access to customers' PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

50. Frontier was at all times fully aware of the obligation to protect the PII of customers, as demonstrated by the existence of its Privacy Policy. Frontier was also aware of the significant repercussions that would result from their its failure to do so.

E. Frontier failed to comply with industry standards.

information.pdf.

[11] *Id.*

51. Large, prominent companies like Frontier are particularly vulnerable to cyberattacks because of the sensitive nature of the information that they collect and maintain. Because of this vulnerability, and because of the frequency and scale of data breaches in recent years, companies like Frontier that routinely handle and maintain sensitive customer information should, at a minimum, implement industry best practices.

52. These practices include educating and training employees; requiring strong passwords and multi-factor authentication for employees and users; implementing multi-layer security like firewalls, antivirus programs, and anti-malware software; limiting access to sensitive data; backing up and encrypting data; setting up network firewalls; monitoring and limiting network ports; and monitoring and limiting access to physical security systems.

53. Upon information and belief Frontier failed to meet the minimum standards of one or more of the following frameworks laying out industry best practices: the NIST Cybersecurity Framework Version 1.1 (including at a minimum 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-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.

54. These frameworks represent the established industry norms for data security, and Frontier's failure to adhere to these widely accepted standards caused the Data Breach and has provided an avenue for criminal exploitation.

F. Plaintiff and the Class suffered and face substantial risk of future injuries because Frontier failed to protect their private information.

55. As a result of Frontier's failure to implement and adhere to security measures that would have protected their PII, Frontier customer PII is now in the hands of criminals, thieves,

and other potentially malicious individuals. Consequently, Plaintiff and the Class Members are at an elevated risk of identity theft, financial fraud, and other identity-related fraud into the indefinite future.

56. Once PII is exposed, it is nearly impossible to ensure the information is fully recovered or protected from future misuse. Thus, Plaintiffs and the Class Members must now immediately allocate time, energy, and money to: (1) closely monitor their bills, records, and credit and financial accounts; (2) change login and password information on sensitive accounts more frequently; (3) rigorously screen phone calls, emails, and other communications to avoid social engineering or spear phishing attacks; and (4) search for and subscribe to suitable identity theft protection and credit monitoring services. Plaintiffs and the Class Members will need to maintain these heightened protective measures for years, possibly their entire lives, due to Frontier's actions.

57. Time is a compensable and valuable resource in the United States, and American adults have only 36 to 40 hours of "leisure time" outside of work per week. Usually this time can be spent at the option of the consumer, but Plaintiff and the Class Members now must spend their leisure time self-monitoring accounts, communicating with financial institutions and credit reporting agencies, contacting government agencies, researching identity protection measures, and implementing self-protection measures that Frontier did not offer

58. Plaintiff and the Class members have also lost the inherent value of their PII and the value of their bargain with Frontier.

59. PII is a valuable property right. Due to its significant value and the prevalence of large-scale data breaches, identity thieves and cybercriminals have openly posted credit card numbers, Social Security numbers, PII, and other sensitive information on various internet

websites, making it publicly accessible. Information from multiple breaches, including the Data Breach, can be aggregated, increasing its value to thieves and amplifying the potential harm to victims.

60. PII can be sold at prices exceeding $1,000.[12] A stolen credit or debit card number can sell for $15 to $110 on the Dark Web.[13] Criminals can also purchase access to entire company data breaches for an average cost of between $2,000 to $4,000.[14]

61. Law-abiding consumers place a high value on the privacy of that data. Researchers shed light on how many consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[15]

62. Accordingly, any company that conducts business with a consumer and subsequently compromises the privacy of their PII effectively deprives that consumer of the full monetary value of their transaction with the company.

63. In sum, due to Frontier's failures, Plaintiffs and the Class Members face a substantial risk of suffering identity theft, fraud, and misuse of their PII, including but not limited to: (a) damage to and diminution in the value of their PII, a form of property that Frontier

---

[12] Ryan Smith, *Revealed – How much is Personal information worth on the dark web?*, Insurance News (May 1, 2023), https://www.insurancebusinessmag.com/us/news/breaking-news/revealed--how-much-is-personal-information-worth-on-the-dark-web-444453.aspx.
[13] Miklos Zoltan, *Dark Web Price Index 2023*, Privacy Affairs (April 23, 2023), https://www.privacyaffairs.com/dark-web-price-index-2023/.
[14] Kaspersky, *Cybercriminals sell access to companies via the Dark Web from $2000* (June 15, 2022), https://www.kaspersky.com/about/press-releases/2022_cybercriminals-sell-access-to-companies-via-the-dark-web-from-2000.
[15] Janice Y. Tsai et al., The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study, 22(2) Information Systems Research 254 (June 2011), accessible at https://www.jstor.org/stable/23015560?seq=1.

obtained from Plaintiffs and the Class, and loss of their bargain with Frontier; (b) violation of their privacy rights; and (c) ongoing and increased risk of identity theft and fraud, which they must spend time and money mitigating. They have had personal and sensitive PII including, reportedly, credit scores and social security numbers, exposed to the public, resulting in ongoing emotional pain, mental anguish, and embarrassment.

CLASS ACTION ALLEGATIONS

64. Plaintiff repeats and realleges each and every fact, matter, and allegation set forth above and incorporates them at this point by reference as though set forth in full.

65. Plaintiff brings this action on behalf of himself and the members of the proposed Class, which consists of:

> **All individuals residing in the United States whose personal identifiable information was compromised in the Data Breach.**

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

67. Plaintiff reserves the right to amend the above definition or to propose subclasses before the Court determines whether certification is appropriate.

68. **Numerosity**: The proposed Class is so numerous that joinder of all members is impracticable. Frontier has acknowledged that the number of class members is at least 751,000.

69. **Typicality**: Plaintiff's claims are typical of the claims of the Class. Plaintiff and all members of the Class were injured through Frontier's uniform misconduct. The same event and conduct that gave rise to Plaintiff's claims are identical to those that give rise to the claims of

every other Class member because Plaintiff and each member of the Class had their sensitive PII compromised in the same way by the same conduct of Frontier.

70. **Adequacy**: Plaintiff is an adequate representative of the Class because Plaintiff's interests do not conflict with the interests of the Class; Plaintiff has retained competent counsel who are experienced in prosecuting complex class action and data breach class action litigation; and Plaintiff and Plaintiff's counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and Plaintiff's counsel.

71. **Superiority**: A class action is superior to all other available methods for the fair and efficient adjudication of this lawsuit because individual litigation of the claims of all members of the Class is economically unfeasible and procedurally impracticable. The injury suffered by each individual member of the Class is relatively small in comparison to the burden and expense of individual prosecution of litigation. It would be very difficult for members of the Class to effectively redress Frontier's wrongdoing. Further, individualized litigation presents a potential for inconsistent or contradictory judgments.

72. **Commonality and Predominance**: There are numerous questions of law and fact common to the Class which predominate over any questions affecting only individual members of the Class.

73. Among the questions of law and fact common to the Class are:

- Whether Frontier engaged in the wrongful conduct alleged herein;
- Whether Frontier failed to adequately safeguard Plaintiff's and the Class's PII;
- Whether Frontier owed a duty to Plaintiff and the Class to adequately protect their PII, and whether it breached this duty;

- Whether Frontier's conduct, including its failure to act, resulted in or was the proximate cause of the breach;
- Whether Frontier was negligent in permitting unauthorized access to Plaintiff's and the Class's PII;
- Whether Frontier was negligent in failing to adhere to reasonable retention policies, thereby greatly increasing the size of the Data Breach;
- Whether Frontier failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiff and the Class;
- Whether Frontier continues to breach duties to Plaintiff and the Class;
- Whether Plaintiff and the Class suffered injury as a proximate result of Frontier's negligent actions or failures to act; and
- Whether Plaintiff and the Class are entitled to recover damages, equitable relief, and other relief.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On behalf of Plaintiff and the CLass)

74. Plaintiff repeats and realleges each and every fact, matter, and allegation set forth above and incorporates them at this point by reference as though set forth in full.

75. Frontier owed a duty of care to Plaintiff and the Class Members to use reasonable means to secure and safeguard the entrusted PII, to prevent its unauthorized access and disclosure, to guard it from theft, and to detect any attempted or actual breach of its systems, as alleged

herein. These common law duties existed because Plaintiff and the Class Members were the foreseeable and probable victims of any inadequate security practices in Frontier's affirmative development and maintenance of its data security systems and its hiring of third-party providers entrusted with accessing, storing, safeguarding, handling, collecting, and/or protecting Plaintiff's and the Class Members' PII. In fact, not only was it foreseeable that Frontier and the Class Members would be harmed by the failure to protect their PII because hackers routinely attempt to steal such information and use it for nefarious purposes, Frontier also knew that it was more likely than not that Plaintiff and other Class Members would be harmed by such exposure and theft of their PII.

76. Frontier's duties to use reasonable security measures also arose as a result of a special relationship with Plaintiff and the Class Members as a result of being entrusted with their PII, which provided an independent duty of care. Plaintiff's and the Class Members' PII was entrusted to Frontier based on the understanding that Frontier would take adequate security precautions. Moreover, Frontier was capable of protecting its network and systems, and the PII it stored on them, from unauthorized access, but failed to do so.

77. Frontier breached its duties when it failed to use security practices that would protect the PII provided to it by Plaintiff and the Class Members, thus resulting in unauthorized exposure and access to their PII.

78. Frontier further breached its duties by failing to design, adopt, implement, control, manage, monitor, update, and audit its processes, controls, policies, procedures, and protocols to comply with the applicable laws and safeguard and protect Plaintiff's and the Class Members' PII within its possession, custody, and control.

79. As a direct and proximate cause of Frontier's failure to use appropriate security

practices and failure to select a third-party provider with adequate data security measures, Plaintiff's and the Class Members' PII was exposed, disseminated, and made available to unauthorized third parties.

80. Frontier admitted that Plaintiff's and the Class Members' PII was wrongfully disclosed as a result of the Data Breach.

81. But for Frontier's wrongful and negligent breach of its duties owed to Plaintiff and the Class Members, their PII would not have been compromised.

82. Neither Plaintiff nor Class members contributed to the Data Breach or subsequent misuse of their PII as described in this Complaint.

83. The Data Breach caused direct and substantial damages to Plaintiff and the Class Members, as well as the likelihood of future and imminent harm through the dissemination of their PII and the greatly enhanced risk of credit fraud and identity theft.

84. As a direct and proximate result of Frontier's negligence, Plaintiff and the Class Members have been injured and are entitled to damages in an amount to be proven at trial. Their injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach investigating the nature of the Data Breach not fully disclosed by Frontier, reviewing bank statements, payment card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost benefit of their bargains and overcharges for

services; and other economic and non-economic harm.

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

85. Plaintiff repeats and realleges each and every fact, matter, and allegation set forth above and incorporates them at this point by reference as though set forth in full.

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

87. Frontier violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect PII and not complying with industry standards. Frontier's conduct was particularly unreasonable given the nature and amount of PII obtained and stored and the foreseeable consequences of a data breach.

88. Frontier's violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence *per se*.

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

90. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of Frontier's failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and the Class Members.

91. As a direct and proximate result of Frontier's negligence, Plaintiff and the Class Members have been injured and are entitled to damages in an amount to be proven at trial. Their

injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach investigating the nature of the Data Breach not fully disclosed by Frontier, reviewing bank statements, payment card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

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

92. Plaintiff repeats and realleges each and every fact, matter, and allegation set forth above and incorporates them at this point by reference as though set forth in full.

93. Plaintiff and the Class Members entered into contracts with Frontier when they obtained products or services from Frontier, or otherwise provided PII to Frontier.

94. As part of these transactions, Frontier agreed to safeguard and protect the PII of Plaintiff and the Class Members.

95. Frontier expressly promised to Plaintiff and the Class Members that it:

- Would use reasonable technical, administrative, and physical safeguards to protect against unauthorized access to, use of, or disclosure of the personal information that Frontier collects and stores;
- Would retain records only as long as reasonably necessary for business,

accounting, or tax purposes; and

- Would *only* share consumers' personal information, including PII, with specified third parties. Apart from the uses laid out in the Privacy Policy, Frontier promises that "We do not otherwise share your personal information."

96. These promises to Plaintiff and the Class Members formed the basis of the bargain between Plaintiff and the Class Members, on the one hand, and Frontier, on the other.

97. Plaintiff and the Class Members would not have provided their PII to Frontier had they known that Frontier would not safeguard their PII.

98. Plaintiff and the Class Members fully performed their obligations under their contracts with Frontier. But Frontier breached its contracts with Plaintiff and the Class Members by failing to safeguard Plaintiff's and the Class Members' PII.

99. As a direct and proximate result of Frontier's breach of implied contract, Plaintiff and the Class Members have been injured and are entitled to damages in an amount to be proven at trial. Their injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as

mitigation measures because of Frontier's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

COUNT IV
***IN THE ALTERNATIVE*—BREACH OF IMPLIED CONTRACT**
(On Behalf of Plaintiff and the Class)

100. Plaintiff repeats and realleges each and every fact, matter, and allegation set forth above and incorporates them at this point by reference as though set forth in full.

101. Plaintiff alleges Count IV in the alternative to Count III.

102. Plaintiff and the Class Members entered into an implied contract with Frontier when they obtained products or services from Frontier, or otherwise provided PII to Frontier.

103. As part of these transactions, Frontier agreed to safeguard and protect the PII of Plaintiff and the Class Members.

104. Plaintiff and the Class Members entered into the implied contracts with the reasonable expectation that Frontier's data security practices and policies were reasonable and consistent with legal requirements and industry standards.

105. Plaintiff and the Class Members would not have provided and entrusted their PII to Frontier in the absence of the implied contract or implied terms between them and Frontier. The safeguarding of the PII of Plaintiff and the Class Members was part of the basis of the parties' bargain.

106. Plaintiff and the Class Members fully performed their obligations under the implied contracts with Frontier.

107. Frontier breached their implied contracts with Plaintiff and the Class Members to protect their PII when they (1) failed to take reasonable steps to use safe and secure systems to protect that information; and (2) allowed the theft of that information by unauthorized third parties.

108. As a direct and proximate result of Frontier's breach of implied contract, Plaintiff and the Class Members have been injured and are entitled to damages in an amount to be proven at trial. Their injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of Frontier's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

COUNT V
IN THE ALTERNATIVE—UNJUST ENRICHMENT
(On behalf of Plaintiff and the Class)

109. Plaintiff repeats and realleges each and every fact, matter, and allegation set forth

above and incorporates them at this point by reference as though set forth in full.

110. Plaintiff alleges Count V in the alternative to Count III above.

111. Plaintiff and the Class Members have an interest, both equitable and legal, in the PII they provided Frontier and that was ultimately stolen in the Data Breach.

112. Frontier benefitted from receiving Plaintiff's and the Class Members' PII, and by its ability to retain, use, sell, and profit from that information. Frontier accepted and was aware of the benefits conferred upon it by Plaintiff and the Class Members.

113. Frontier also understood and appreciated that the PII pertaining to Plaintiff and the Class Members was private and confidential and its value depended upon Frontier maintaining the privacy and confidentiality of that PII except as expressly agreed.

114. But for Frontier's willingness and commitment to maintain its privacy and confidentiality, Plaintiff and the Class Members would not have provided PII to Frontier or would not have permitted Frontier to gather additional PII.

115. Plaintiff's and the Class Members' PII has an independent value to Frontier. Frontier was unjustly enriched by profiting from the additional services and products it was able to market, sell, and create through the use of Plaintiff's and the Class Members' PII.

116. Due to Frontier's actions, Frontier unjustly obtained benefits equivalent to the disparity in value between the payments made for services with reasonable data privacy and security measures, and the services received, which lacked such measures.

117. It is inequitable, unfair, and unjust for Frontier to retain these wrongfully obtained benefits. Frontier's retention of wrongfully obtained monies would violate fundamental principles of justice, equity, and good conscience.

118. The benefit conferred upon, received, and enjoyed by Frontier was not conferred officiously or gratuitously, and it would be inequitable, unfair, and unjust for Frontier to retain the benefit.

119. Frontier's defective security and its unfair and deceptive conduct have, among

other things, caused Plaintiff and the Class Members to unfairly incur substantial time and/or costs to mitigate and monitor the use of their PII and has caused the Plaintiff and the Class Members other damages as described herein.

120. Plaintiff and the Class Members have no adequate remedy at law.

121. Frontier is therefore liable to Plaintiff and the Class Members for restitution or disgorgement in the amount of the benefit conferred on Frontier as a result of its wrongful conduct, including specifically: the value to Frontier of the PII that was stolen in the Data Breach; the profits Frontier received and is receiving from the use of that information; and the amounts that Frontier overcharged Plaintiff and the Class Members for use of Frontier's products and services.

PRAYER FOR RELIEF

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

A. An order certifying this action as a class action under Federal Rule of Civil Procedure 23, defining the Class as requested herein, appointing the undersigned as Class Counsel, and finding that Plaintiff is a proper representative of the proposed Class;

B. For injunctive and other equitable relief as necessary to protect the interests of Plaintiff and the Class;

C. For an award of compensatory, consequential, and general damages, including nominal damages, as allowed by law in an amount to be determined;

D. For an award of restitution or disgorgement, in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as the Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all triable issues.

Dated: June 14, 2024

Respectfully submitted,

By: */s/ Joe Kendall*
Joe Kendall, Texas Bar No. 11260700
KENDALL LAW GROUP, PLLC
3811 Turtle Creek Boulevard, Suite 825
Dallas, TX 75219
Phone: (214) 744-3000
Fax: (214) 744-3015
jkendall@kendalllawgroup.com

Katherine M. Aizpuru (*pro hac vice forthcoming*)
TYCKO & ZAVAREEI LLP
2000 Pennsylvania Avenue, NW, Suite 1010
Washington, D.C. 20006
Phone: (202) 973-0900
kaizpuru@tzlegal.com

Counsel for Plaintiff and the Proposed Class