UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

CHRISTOPHER MILLER, individually and on behalf of all others similarly situated, ***Plaintiff*,** **v.** **FRONTIER COMMUNICATIONS PARENT, INC.,** ***Defendant*.**	Case No. 3:24-cv-01 6 7 1 **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Christopher Miller, ("Plaintiff") brings this Class Action Complaint ("Complaint") against Frontier Communications Parent, Incorporated, ("Defendant") as an individual and on behalf of all others similarly situated, and alleges, upon personal knowledge as to Plaintiff's own actions and to counsels' investigation, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. Plaintiff brings this class action against Defendant Frontier Communications Parent, Inc., for its failure to properly secure and safeguard the personally identifiable information ("PII") of its customers, including, but not limited to: full names, addresses, social security numbers, email addresses, credit scores, phone numbers, and dates of birth.

2. Defendant offers internet, digital television, and telecommunications services to residential and business customers in 25 states. Defendant offers fiber optic television services

(*i.e.,* Frontier Fiber TV) and requires customers to provide their PII prior to purchasing a cable subscription.

3. Defendant's published privacy policy provides, "[w]e 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."[1]

4. On, or about, April 14, 2024, Defendant detected unusual activity on its IT systems and determined that Plaintiff's personal information—which was entrusted to Defendant on the mutual understanding that Defendant would protect it against unauthorized disclosure—was accessed and exfiltrated in a data breach (hereafter referred to as the "Data Breach").

5. On or about June 6, 2024, Defendant sent out a data breach notice letter to Plaintiff and other individuals who were affected by the data breach. In the letter, Defendant offered one (1) year of identity monitoring services and recommended that Plaintiff "remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity."

6. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's PII was a known risk to Defendant, and thus, Defendant was on notice that failing to take steps necessary to secure the PII from those risks left the data in a dangerous condition.

7. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable data protection procedures necessary to protect consumers' PII from a foreseeable and preventable risk of unauthorized disclosure. Had Defendant remedied the vulnerabilities in its

[1] https://frontier.com/corporate/privacy-policy (accessed June 13, 2024).

information technology environment, and implemented administrative, technical, and physical controls consistent with industry best practices, it could have prevented the Data Breach.

8. Defendant's conduct resulted in the unauthorized disclosure of Plaintiff's private information to unknown cybercriminals. The unauthorized disclosure of Plaintiff's PII constitutes an invasion of a legally protected privacy interest, that is traceable to the Defendant's failure to adequately secure the PII in its custody, and has resulted in actual, particularized, and concrete harm to the Plaintiff. Plaintiff suffered actual injury in the form of damages to and diminution in the value of the PII that was compromised as a result of the Data Breach. The injuries Plaintiff suffered, as described herein, can be redressed by a favorable decision in this matter.

9. Defendant has not provided any assurances that: all data acquired in the Data Breach, or copies thereof, have been recovered or destroyed; or, that Defendant has modified its data protection policies, procedures, and practices sufficient to avoid future, similar, data breaches.

10. Defendant's conduct, as evidenced by the circumstances of the Data Breach, has created a substantial risk of future identity theft or fraud. The circumstances demonstrating a substantial risk of future identity theft or fraud, include, but are not limited to:

a. **Sensitive Data Type**: The data acquired in the Data Breach included unencrypted names, addresses, social security numbers, dates of birth, email addresses, credit scores, and phone numbers.[2] Upon information and belief, this information could be used by cybercriminals to perpetuate fraud.

b. **Data Breach Type**: On April 14, 2024, Defendant reported that it discovered an unauthorized third-party targeted its network and exfiltrated the PII of more than 750,000 people. On June 4, 2024, the RansomHub extortion group claimed responsibility for the attack and threatened to leak the customer data it stole unless Defendant paid their ransom demand by June 14, 2024.[3] RansomHub has been responsible for 61 ransomware attacks in the last three (3) months. In all previous attacks, after RansomHub gained unauthorized access to a target

[2] https://www.theverge.com/2024/6/10/24175169/frontier-communications-hack-cyberattack-data-breach-ransom (last accessed June 13, 2024).
[3] *Id.*

network, they deployed a ransomware payload, which exfiltrated sensitive data and encrypted infected PC files. RansomHub then demanded a ransom payment to unencrypt the stolen files. When the target failed to pay the demand, RansomHub either sold or leaked the stolen data on the dark web.[4]

c. **Data Misuse**: On June 14, 2024, RansomHub leaked the data it acquired in the Data Breach on the dark web. The dark web uses a series of encrypted networks to hide users' identities, which makes it convenient for criminals to buy and sell illegally obtained data. Many criminals purchase stolen personal data off the dark web before launching social engineering-based attacks. A social engineering attack is a method of using psychological manipulation to deceive a victim and gain access to a computer system or to steal sensitive information such as login credentials. Social engineering attacks that can be launched using names, telephone numbers and email addresses include phishing, smishing (SMS message), vishing (voice messaging), pretexting, and baiting attacks.

11. The imminent risk of future harm resulting from the Data Breach is traceable to the Defendant's failure to adequately secure the PII in its custody, and has created a separate, particularized, and concrete harm to the Plaintiffs.

12. More specifically, the Plaintiff's exposure to the substantial risk of future identity theft or fraud caused them to: (i) spend money on mitigation measures like credit monitoring services and dark web searches; (ii) uncompensated lost time and effort spent responding to the Data Breach; and/or (iii) experience emotional distress associated with reviewing accounts for fraud, changing usernames and passwords or closing accounts to prevent fraud, and general anxiety over the consequences of the Data Breach. The harm Plaintiff's suffered can be redressed by a favorable decision in this matter.

13. Plaintiff and those similarly situated face a substantial risk of future spam, phishing, or other social engineering attacks where their full names, addresses, email addresses, and phone numbers were stolen by a hacker group (RansomHub), known for stealing and reselling personal data on the dark web. Names, telephone numbers and email addresses can be used by

[4] https://www.theregister.com/2024/06/05/ransomhub_knight_reboot/ (last accessed June 13, 2024).

cybercriminals to launch social engineering attacks designed to trick individuals into giving away sensitive information. Plaintiff has incurred out of pocket costs for purchasing products to protect from phishing, smishing (SMS message), vishing (voice messaging), pretexting, and other social engineering-based attacks.

14. Armed with the PII acquired in the Data Breach, data thieves have already engaged in identity theft and fraud and can, in the future, commit a variety of crimes including, opening new financial accounts, taking out loans, using Plaintiff's information to obtain government benefits, file fraudulent tax returns, obtain driver's licenses, and give false information to police during an arrest.

15. As a result of the Data Breach, Plaintiff suffered injuries including, but not limited to: (i) invasion of privacy; (ii) theft of PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and increased risk their PII will be misused, where: (a) their data remains unencrypted and available for unauthorized third parties to access; and (b) remains backed up under Defendant's possession or control and is subject to further unauthorized disclosures so long as Defendant fails to implement appropriate and reasonable measures to protect the PII.

16. Plaintiff brings this class action lawsuit individually, and on behalf of all those similarly situated, to address Defendant's inadequate protection of PII that it collected and maintained, and for failing to provide timely and adequate notice of the Data Breach.

17. Through this Complaint, Plaintiff seeks to remedy these harms individually, and on behalf of all similarly situated individuals whose PII was accessed during the Data Breach. Plaintiff has a continuing interest in ensuring that their personal information is kept confidential and protected from disclosure, and Plaintiff should be entitled to injunctive and other equitable relief.

JURISDICTION & VENUE

18. 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 $5,000,000.00, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class, including Plaintiff, is a citizen of a state different from Defendant. Plaintiff is a citizen of California. Defendant is a citizen of Texas.

19. This Court has personal jurisdiction over Defendant because its principal place of business is in the Dallas Division of the Northern District of Texas. Defendant has also purposefully availed itself of the laws, rights, and benefits of the State of Texas.

20. Venue is proper under 28 U.S.C §1391(b) because Defendant maintains a principal place of business in the Dallas Division of the Northern District of Texas and a substantial part of the events and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

PARTIES

21. Plaintiff Christopher Miller is a citizen of the State of California. At all relevant times, Plaintiff Miller has been a resident of Long Beach, Los Angeles County.

22. Defendant, Frontier Communications Parent, Incorporated, maintains a principal place of business 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.

FACTUAL ALLEGATIONS

23. Defendant offers cable television services (*i.e.,* Frontier Fiber TV), internet, and telecommunications services and requires customers to provide their PII prior to purchasing a cable, internet, or telephone subscription.

24. Plaintiff and Class Members (later defined) are current and former subscribers of Defendant's various services.

25. In the course of their relationship, subscribers, including Plaintiff and Class Members, provided Defendant with at least the following: full names, dates of birth, contact information, and social security number.

26. Upon information and belief, while collecting PII from subscribers, including Plaintiff and Class Members, Defendant promised to use reasonable technical, administrative, and physical safeguards to protect the personal information it collected. These promises were contained in the applicable privacy policy and through other disclosures in compliance with statutory privacy requirements.

27. Plaintiff and the Class Members, as customers of Defendant, relied on these representations and on this sophisticated business entity to keep their PII confidential, securely maintained, and to make only authorized disclosures of this information.

Data Breaches Are Avoidable

28. On, or about, June 6, 2024, roughly two months after Defendant learned that the Plaintiff's PII was accessed and exfiltrated by cybercriminals, Defendant issued data breach notice letters to the affected individuals.

29. Upon information and belief, the Data Breach was a direct result of Defendant's failure to implement reasonable data protection measures which would protect Plaintiff's and Class Members' PII from the foreseeable and preventable risk of unauthorized disclosure.

30. Upon information and belief, the Data Breach occurred as the result of a ransomware attack. In a ransomware attack the attackers use software to encrypt data on a compromised network, rendering it unusable and then demand payment to restore control over the network.[5] Ransomware groups frequently implement a double extortion tactic, "where the cybercriminal posts portions of the data to increase their leverage and force the victim to pay the ransom, and then sells the stolen data in cybercriminal forums and dark web marketplaces for additional revenue."[6]

31. To prevent and detect cyber-attacks and/or ransomware attacks, Defendant could and should have implemented the following measures:

Reasonable Protective Measures

a. Regularly patch critical vulnerabilities in operating systems, software, and firmware on devices. Consider using a centralized patch management system.
b. Check expert websites (such as www.us-cert.gov) and your software vendors' websites regularly for alerts about new vulnerabilities and implement policies for installing vendor-approved patches to correct problems.
c. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks. Depending on your circumstances, appropriate assessments may range from having a knowledgeable employee run off-the-shelf security software to having an independent professional conduct a full-scale security audit.
d. Scan computers on your network to identify and profile the operating system and open network services. If you find services that you don't need, disable them to prevent hacks or other potential security problems.

[5] *Ransomware FAQs*, https://www.cisa.gov/stopransomware/ransomware-faqs (accessed June 11, 2024).
[6] *Ransomware: The Data Exfiltration and Double Extortion Trends*, https://www.cisecurity.org/insights/blog/ransomware-the-data-exfiltration-and-double-extortion-trends (accessed June 11, 2024).

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

f. Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email.

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

h. Configure firewalls to block access to known malicious IP addresses.

i. Set anti-virus and anti-malware programs to conduct regular scans automatically.

j. Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

k. Configure access controls—including file, directory, and network share permissions— with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

l. Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

m. Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

n. Consider disabling Remote Desktop protocol (RDP) if it is not being used.

o. Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

p. Execute operating system environments or specific programs in a virtualized environment.

q. Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.

r. Conduct an annual penetration test and vulnerability assessment.

s. Secure your backups.[7]

t. Identify the computers or servers where sensitive personal information is stored.

u. Identify all connections to the computers where you store sensitive information. These may include the internet, electronic cash registers, computers at your branch offices, computers used by service providers to support your network, digital copiers, and wireless devices like smartphones, tablets, or inventory scanners.

---

[7] *How to Protect Your Networks from Ransomware*, at p.3, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (accessed June 11, 2024).

v. Don't store sensitive consumer data on any computer with an internet connection unless it's essential for conducting your business.

w. Encrypt sensitive information that you send to third parties over public networks (like the internet) and encrypt sensitive information that is stored on your computer network, laptops, or portable storage devices used by your employees. Consider also encrypting email transmissions within your business.

x. Regularly run up-to-date anti-malware programs on individual computers and on servers on your network.

y. Restrict employees' ability to download unauthorized software. Software downloaded to devices that connect to your network (computers, smartphones, and tablets) could be used to distribute malware.

z. To detect network breaches when they occur, consider using an intrusion detection system.

aa. Create a "culture of security" by implementing a regular schedule of employee training. Update employees as you find out about new risks and vulnerabilities.

bb. Tell employees about your company policies regarding keeping information secure and confidential. Post reminders in areas where sensitive information is used or stored, as well as where employees congregate.

cc. Teach employees about the dangers of spear phishing—emails containing information that makes the emails look legitimate. These emails may appear to come from someone within your company, generally someone in a position of authority. Make it office policy to independently verify any emails requesting sensitive information.

dd. Before you outsource any of your business functions investigate the company's data security practices and compare their standards to yours.[8]

32. Given that Defendant stored the PII of its current and former customers, Defendant could and should have implemented all the above measures to prevent and detect cyberattacks. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of Plaintiff's and the Class Members' PII.

[8] *Protecting Personal Information: A Guide for Business*, https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (accessed June 11, 2024).

33. Defendant knew and understood unencrypted PII is valuable and highly sought after by cybercriminals seeking to illegally monetize that data. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding customer PII and of the foreseeable consequences that would occur if Defendant's network was breached, including the significant cost that would be imposed on Plaintiff and the Class Members as a result.

Plaintiff and Class Members Sustained Damages in the Data Breach

34. The invasion of the Plaintiff's and Class Members' privacy suffered in this Data Breach constitutes a redressable injury.

35. Additionally, Plaintiff and Class Members face a substantial risk of future identity theft or fraud where their names, social security numbers, and dates of birth were targeted by a sophisticated hacker group known for stealing and reselling sensitive data on the dark web.

36. Furthermore, Plaintiff and Class Members face a substantial risk of future spam, phishing, or other social engineering attacks where their full names and contact information were stolen and subsequently released on the dark web.

37. Upon information and belief, RansomHub has acquired enough personal information for a criminal to be able to open a bank account or commit other fraud using the information stolen in the Data Breach. A criminal can easily link data acquired in the data breach with information available from other sources to commit a variety of identity theft related crimes.

38. An example of criminals piecing together bits and pieces of data is the development of "Fullz" packages.[9] With "Fullz" packages, cyber-criminals can cross-reference two sources of

[9] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials,

PII to marry data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

39. Given the type of targeted attack in this case, the sophistication of the criminal claiming responsibility for the Data Breach, the hacker group's behavior in prior data breaches, and the type of PII involved in the Data Breach, there is a substantial probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for purchase by criminals intending to utilize the PII for identity theft crimes.

40. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records. Several federal and state agencies have recommended steps that data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[10]

41. Consequently, Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions to understand and mitigate the effects of the Data Breach. Additionally, the retail cost of credit monitoring and identity theft monitoring can cost

---

commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texaslife-insurance.

[10] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps

around $200 a year. The cost of dark web scanning and monitoring services can cost around $180 per year.

42. Personal information is of great value, in 2019, the data brokering industry was worth roughly $200 billion.[11] Data such as name, address, phone number, and credit history has been sold at prices ranging from $40 to $200 per record.[12] Sensitive PII can sell for as much as $363 per record.[13]

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

44. Given these facts, by transacting business with Plaintiff and Class Members, collecting their PII, using their PII to market additional products and services, and then permitting the unauthorized disclosure of their PII has deprived Plaintiff and Class Members of the benefit of their bargain with Defendant.

45. Furthermore, Defendant's poor data security practices deprived Plaintiff and Class Members of the benefit of their bargain. When agreeing to pay Defendant for products or services,

---

[11] *Column: Shadowy data brokers make the most of their invisibility cloak*, https://www.latimes.com/business/story/2019-11-05/column-data-brokers

[12] *In the Dark*, VPNOverview, 2019, available at: https://vpnoverview.com/privacy/anonymousbrowsing/in-the-dark/

[13] *See, e.g.,* John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

customers understood and expected that they were, in part, paying for the protection of their personal data, when in fact, Defendant did not provide adequate security. Accordingly, Plaintiff and Class Members received services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

46. Through this Complaint, Plaintiff seeks redress for the damages and injuries that resulted from the Data Breach.

CLASS ALLEGATIONS

47. Plaintiff brings this nationwide class action individually, and on behalf of all similarly situated individuals, pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

48. The Class that Plaintiff seeks to represent is defined as follows:

Nationwide Class

All individuals residing in the United States whose PII was accessed and acquired by an unauthorized party as a result of a data breach that occurred on, or about, April 14, 2024, as reported by Defendant Frontier Communications Parent, Inc., (the "Class").

California Subclass

All individuals residing in California whose PII was accessed and acquired by an unauthorized party as a result of the Data Breach as reported by Defendant Frontier Communications Parent, Inc., (the "California Subclass").

Fiber TV Subclass

All individuals residing in the United States who purchased cable subscription services from Defendant Frontier Communications Parent, Inc., and whose PII was accessed and acquired by an unauthorized party as a result of the Data Breach (the "Fiber TV Subclass").

49. Collectively, the Class, California Subclass, and Fiber TV Subclass are referred to as the "Classes" or "Class Members."

50. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded

from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

51. Plaintiff reserves the right to amend the definitions of the Classes or add a Class or Subclass if further information and discovery indicate that the definitions of the Classes should be narrowed, expanded, or otherwise modified.

52. Numerosity: The members of the Classes are so numerous that joinder of all members is impracticable, if not completely impossible. The members of the Classes are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time and such number is exclusively in the possession of Defendant, upon information and belief, millions of individuals were impacted in Data Breach.

53. Common questions of law and fact exist as to all members of the Classes and predominate over any questions affecting solely individual members of the Classes. Among the questions of law and fact common to the Classes that predominate over questions which may affect individual Class Members, including the following:

a. Whether and to what extent Defendant had a duty to protect the PII of Plaintiff and Class Members;
b. Whether Defendant had respective duties not to disclose the PII of Plaintiff and Class Members to unauthorized third parties;
c. Whether Defendants had respective duties not to use the PII of Plaintiff and Class Members for non-business purposes;
d. Whether Defendant failed to adequately safeguard the PII of Plaintiff and Class Members;
e. Whether and when Defendants actually learned of the Data Breach;
f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;
g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;

h. 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;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Plaintiff and Class Members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Defendant's wrongful conduct;

k. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and ongoing harm faced as a result of the Data Breach.

54. Typicality: Plaintiff's claims are typical of those of the other members of the Classes because Plaintiff, like every other Class Member, was exposed to virtually identical conduct and now suffers from the same violations of the law as each other member of the Classes.

55. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant acted or refused to act on grounds generally applicable to the Classes, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Classes as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenges of these policies hinges on Defendant's conduct with respect to the Classes as a whole, not on facts or law applicable only to Plaintiff.

56. Adequacy: Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiff seeks no relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex class action and data breach litigation, and Plaintiff intends to prosecute this action vigorously.

57. Superiority and Manageability: The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other

available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

58. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since Defendant would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Classes and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

59. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

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

61. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII of Classes, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

62. Further, Defendant has acted on grounds that apply generally to the Classes as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class- wide basis.

63. Likewise, particular issues under Rule 42(d)(1) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant failed to timely notify the Plaintiff and the Classes of the Data Breach;
b. Whether Defendant owed a legal duty to Plaintiff and the Classes to exercise due care in collecting, sharing, storing, and safeguarding their PII;
c. Whether Defendant's (or their vendors') security measures to protect its network were reasonable in light of industry best practices;
d. Whether Defendant's (or their vendors') failure to institute adequate data protection measures amounted to negligence;
e. Whether Defendant failed to take commercially reasonable steps to safeguard consumer PII;
f. Whether Defendant made false representations about their data privacy practices and commitment to the security and confidentiality of customer information; and
g. Whether adherence to FTC recommendations and best practices for protecting personal information would have reasonably prevented the Data Breach.

CAUSES OF ACTION

COUNT 1: VIOLATION OF THE CABLE COMMUNICATIONS PRIVACY ACT (47 U.S.C. §551)
(On behalf of Plaintiff and the Classes)

64. Plaintiff re-alleges and incorporates by reference all the allegations contained in the foregoing paragraphs as if fully set forth herein.

65. Defendant is a cable operator, who provides video programming to subscribers via fiber optic cables (*i.e.,* Frontier Fiber TV), over a cable system, as defined under the Cable Communications Privacy Act of 1984.

66. Plaintiff entered into an agreement with Defendant to provide cable service and other services on a subscription basis. During the course of the relationship, Defendant collected the personally identifiable information of its subscribers, including the Plaintiff and the Classes, to render the contracted cable television service and other video programming services.

67. Defendant had a duty to: (i) not disclose personally identifiable information concerning any subscriber without the prior written or electronic consent of the subscriber concerned; (ii) take such actions as are necessary to prevent unauthorized access to such information by a person other than the subscriber; and, (iii) destroy personally identifiable information when the information is no longer necessary for the purpose for which it was collected and there are no pending requests or orders for access to such information.

68. On, or about, April 14, 2024, Defendant disclosed the Plaintiff's and Class Members' PII without their authorization. Such unauthorized disclosure was the direct result of Defendant's failure to take such actions as were necessary to prevent unauthorized access to such information, including, but not limited to:

a. Failing to implement organizational controls, including a patch management policy to track and manage updates and patches for known vulnerabilities.

b. Failing to have defined periods when patches must be installed and/or an automated means of determining what patches are needed, where they are needed, and the status of current patch levels by location.

c. Failing to encrypt personally identifying information in transit and at rest.

d. Failing to adopt, implement, and maintain adequate security measures to safeguard PII.

e. Failing to implement data security practices consistent with Defendant's published privacy policies.

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

g. Allowing unauthorized access to subscribers' PII.

h. Failing to detect, in a timely manner, that Class Members' PII had been compromised.

i. Failing to remove former subscribers' PII it was no longer required to retain.

j. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

69. Upon information and belief, the Data Breach occurred because of Defendant's failure to remedy a vulnerability in Microsoft's netlogon remote protocol. The specific vulnerability was announced on August 11, 2020, and it was identified as having a "critical" severity level. Accordingly, Defendant's failure to take such actions as were necessary to prevent unauthorized access to Plaintiff's and Class Members' PII—namely, Defendant's failure to fix a critical vulnerability—existed for 1,343 days (3 years, 8 months, and 4 days). Under the circumstances, such failure to remedy a known, *critical*, vulnerability constitutes recklessness, wanton misconduct, or willful negligence.

70. As a direct and proximate result of Defendant's failure to prevent unauthorized access to, and disclosure of, its subscriber's PII, Plaintiff and Class Members personal data was acquired in the Data Breach.

71. Plaintiff and Class Members were within the class of persons the Cable Communications Privacy Act was intended to protect and the type of harm that resulted from the Data Breach was the type of harm the statute was intended to guard against.

72. As a direct and proximate result of the Defendant's failure to comply with the Cable Communications Privacy Act of 1984, Plaintiff and Class Members suffered injuries including, but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and increased risk their PII will be misused, where: (a) their data remains unencrypted and available for unauthorized third parties to access; and (b) remains backed up under Defendant's possession or control and is subject to further unauthorized disclosures so long as Defendant fails to implement appropriate and reasonable measures to protect the PII.

73. Plaintiff and Class Members are entitled to: (i) actual damages, but not less than liquidated damages computed at the rate of $100 a day for each day of violation or $1,000, whichever is higher; (ii) punitive damages; and (iii) attorneys' fees and other litigation costs.

74. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data protection procedures; (ii) patch all critical vulnerabilities; and (iii) to provide adequate credit monitoring to all affected by the Data Breach.

COUNT 2: NEGLIGENCE/NEGLIGENCE *PER SE*
(On behalf of Plaintiff and the Classes)

75. Plaintiff re-alleges and incorporates by reference all the allegations contained in the foregoing paragraphs as if fully set forth herein.

76. Defendant requires their customers, including Plaintiff and Class Members, to submit PII in the ordinary course of providing cable television services.

77. Defendant gathered and stored the PII of Plaintiff and Class Members as part of its business of soliciting its services to customers. Plaintiff and Class Members entrusted Defendant with their PII with the understanding that Defendant would adequately safeguard their information.

78. Defendant had full knowledge of the types of PII it collected and the types of harm that Plaintiff and Class Members would suffer if that data was accessed and exfiltrated by an unauthorized third-party.

79. By collecting, storing, sharing, and using the Plaintiff's and Class Members' PII for commercial gain, Defendant assumed a duty to use reasonable means to safeguard the personal data it obtained.

80. Defendant's duty included a responsibility to ensure it: (i) implemented reasonable administrative, technical, and physical measures to detect and prevent unauthorized intrusions into its information technology environment; (ii) contractually obligated its vendors to adhere to the requirements of Defendant's privacy policy; (iii) complied with applicable statutes and data protection obligations; (iv) conducted regular privacy assessments and security audits; (v) regularly audited for compliance with contractual and other applicable data protection obligations; and, (vi) provided timely notice to individuals impacted by a data breach event.

81. Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits unfair or deceptive trade practices that affect commerce. Deceptive practices, as interpreted by the FTC, include failing to adhere to a company's own stated privacy policies.

82. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former subscribers' PII that Defendant was no longer required to retain.

83. Defendant had a duty to notify Plaintiff and the Classes of the Data Breach promptly and adequately. Such notice was necessary to allow Plaintiff and the Classes to take steps to prevent, mitigate, and repair any fraudulent usage of their PII.

84. Defendant violated Section 5 of the FTC Act by failing to adhere to its own privacy policy[14] regarding the confidentiality and security of Plaintiff and Class Members information. Defendant further violated Section 5 of the FTC Act, and other state consumer protection statutes by failing to use reasonable measures to protect PII. Defendant's violations of Section 5 of the FTC Act, and other state consumer protection statutes, constitutes negligence *per se.*

85. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' PII. The specific negligent acts and omissions committed by Defendant includes, but are not limited to, the following:

a. Failing to implement organizational controls, including a patch management policy to track and manage updates and patches for known vulnerabilities.

b. Failing to have defined periods when patches must be installed and/or an automated means of determining what patches are needed, where they are needed, and the status of current patch levels by location.

c. Failing to encrypt personally identifying information in transit and at rest.

d. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII.

e. Failing to adequately monitor the security of their networks and systems.

f. Allowing unauthorized access to PII.

g. Failing to detect in a timely manner that PII had been compromised.

h. Failing to remove former customers' PII it was no longer required to retain.

[14] Frontier Communications Privacy Policy, available here: https://frontier.com/corporate/privacy-policy

i. Failing to timely and adequately notify Plaintiff and Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

j. Failing to implement data security practices consistent with Defendant's published privacy policies.

86. Plaintiff and Class Members were within the class of persons the Federal Trade Commission Act was intended to protect and the type of harm that resulted from the Data Breach was the type of harm the statue was intended to guard against.

87. The injuries resulting to Plaintiff and the Classes because of Defendant's failure to use adequate security measures was reasonably foreseeable.

88. Plaintiff and the Class were the foreseeable victims of a data breach. Defendant knew or should have known of the inherent risks in collecting and storing PII, the critical importance of protecting that PII, and the necessity of updating, patching, or fixing critical vulnerabilities in its network.

89. Plaintiff and the Classes had no ability to protect the PII in Defendant's possession. Defendant was in the best position to protect against the harms suffered by Plaintiff and the Classes as a result of the Data Breach.

90. But for Defendant's breach of duties owed to Plaintiff and the Classes, their PII would not have been compromised. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiff and the Classes and the harm, or risk of imminent harm, suffered by Plaintiff and the Classes.

91. As a result of the Data Breach, Plaintiff and Class Members suffered injuries including, but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs

associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and increased risk their PII will be misused, where: (a) their data remains unencrypted and available for unauthorized third parties to access; and (b) remains backed up under Defendant's possession or control and is subject to further unauthorized disclosures so long as Defendant fails to implement appropriate and reasonable measures to protect the PII.

92. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

93. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to: (i) strengthen its data protection procedures; (ii) patch all critical vulnerabilities; and (iii) to provide adequate credit monitoring to all affected by the Data Breach.

COUNT 3: BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiff and the Classes)

94. Plaintiff re-alleges and incorporates by reference all the allegations contained in the foregoing paragraphs as if fully set forth herein.

95. Defendant requires their customers, including Plaintiff and Class Members, to submit PII in the ordinary course of providing cable television services. Defendant published a privacy policy to inform subscribers about how Defendant collects, uses, shares, and protects the information Defendant gathers in connection with the provision of cable television services.

96. In so doing, Plaintiff and Class Members entered implied contracts with Defendant by which Defendant agreed to "use reasonable technical, administrative, and physical safeguards

to protect against unauthorized access to, use of, or disclosure of the personal information" it collects and stores.[15]

97. Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of an expressed or implied promise to implement reasonable data protection measures.

98. Plaintiff and Class Members fully and adequately performed their obligations under the implied contract with Defendant.

99. Defendant breached the implied contract with Plaintiff and Class Members which arose from the course of conduct between the parties, as well as disclosures on the Defendant's web site, privacy policy, and in other documents, all of which created a reasonable expectation that the personal information Defendant collected would be adequately protected and that the Defendant would take such actions as were necessary to prevent unauthorized access to, use of, or disclosure of such information.

100. As a direct and proximate result of the Defendant's breach of an implied contract, Plaintiff and Class Members suffered injuries including, but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and increased risk their PII will be misused, where: (a) their data remains unencrypted and available for unauthorized third parties to access; and (b) remains backed up under Defendant's possession or control and is subject

[15] *See*, Frontier Communications Privacy Policy, *How We Protect Your Information*, https://frontier.com/corporate/privacy-policy

to further unauthorized disclosures so long as Defendant fails to implement appropriate and reasonable measures to protect the PII.

101. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to: (i) strengthen its data protection procedures; (ii) patch all critical vulnerabilities; and (iii) to provide adequate credit monitoring to all affected by the Data Breach.

COUNT 4: UNJUST ENRICHMENT
(On behalf of Plaintiff and the Classes)

102. Plaintiff realleges and incorporates by reference all the allegations contained in the foregoing paragraphs, as if fully set forth herein.

103. Plaintiff brings this Count in the alternative to the breach of implied contract count above.

104. By providing their PII, Plaintiff and Class Members conferred a monetary benefit on Defendant. Defendant knew that Plaintiff and Class Members conferred a benefit upon them and have accepted and retained that benefit. Defendant used the data to market, advertise, and sell additional services to Plaintiff and Class Members.

105. By collecting the PII, Defendant was obligated to safeguard and protect such information, to keep such information confidential, and to timely and accurately notify Plaintiff and Class Members if their data had been compromised or stolen.

106. Defendant failed to secure Plaintiff's and Class Members' PII and, therefore, it would be unjust for Defendant to retain any of the benefits that Plaintiff and Class Members conferred upon Defendant without paying value in return.

107. As a direct and proximate result of the Defendant's conduct, Plaintiff and Class Members suffered injuries including, but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with

attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and increased risk their PII will be misused, where: (a) their data remains unencrypted and available for unauthorized third parties to access; and (b) remains backed up under Defendant's possession or control and is subject to further unauthorized disclosures so long as Defendant fails to implement appropriate and reasonable measures to protect the PII.

108. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendant from its wrongful conduct.

COUNT 5: INVASION OF PRIVACY
(On behalf of Plaintiff and the Classes)

109. Plaintiff realleges and incorporates by reference all the allegations contained in the foregoing paragraphs, as if fully set forth herein.

110. Plaintiff and Class Members had a legitimate expectation of privacy in their personally identifying information such as social security numbers, dates of birth, and credit scores. Plaintiff and Class Members were entitled to the protection of this information from disclosure to unauthorized third parties.

111. Defendant owed a duty to their current, former, and prospective customers, including Plaintiff and Class Members, to keep their PII confidential.

112. Defendant permitted the public disclosure of Plaintiff's and Class Members' PII to unauthorized third parties.

113. The PII that was disclosed without the Plaintiff's and Class Members' authorization was highly sensitive, private, and confidential. The public disclosure of the type of PII at issue here would be highly offensive to a reasonable person of ordinary sensibilities.

114. Defendant permitted its information technology environment to remain vulnerable to foreseeable threats, which created an atmosphere for the Data Breach to occur. Despite knowledge of the substantial risk of harm created by these conditions, Defendant intentionally disregarded the risk, thus permitting the Data Breach to occur.

115. By permitting the unauthorized disclosure, Defendant acted with reckless disregard for the privacy of Plaintiff and Class Members, and with knowledge that such disclosure would be highly offensive to a reasonable person. Furthermore, the disclosure of the PII at issue was not newsworthy or of any service to the public interest.

116. Defendant was aware of the potential of a data breach and failed to adequately safeguard its systems and/or implement appropriate policies and procedures to prevent the unauthorized disclosure of Plaintiff's and Class Members' data.

117. Defendant acted with such reckless disregard as to the safety of Plaintiff's and Class Members' PII to rise to the level of intentionally allowing the intrusion upon the seclusion, private affairs, or concerns of Plaintiff and Class Members.

118. Plaintiff and Class Members have been damaged by the invasion of their privacy in an amount to be determined at trial.

COUNT 6: DECLARATORY JUDGMENT
(On behalf of Plaintiff and the Classes)

119. Plaintiff re-alleges and incorporates by reference the paragraphs above as if fully set forth herein.

120. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the statutes described in this Complaint.

121. An actual controversy has arisen in the wake of Defendant's data breach regarding its present and prospective common law and other duties to reasonably safeguard its customers' PII and whether Defendant is currently maintaining data security measures adequate to protect consumers from further unauthorized disclosures of their PII.

122. Plaintiff alleges that Defendant's data security measures remain inadequate. Plaintiff will continue to suffer injury as a result of the compromise of their PII and remain at imminent risk that further compromises of their PII will occur in the future.

123. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant continues to owe a legal duty to secure current and former customers' PII and to timely notify them of a data breach under the common law, Section 5 of the FTC Act, and various state statutes.

b. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure Plaintiff and Class Members' PII.

124. The Court also should issue corresponding prospective injunctive relief requiring that Defendant employs adequate data protection practices consistent with law and industry standards.

125. If an injunction is not issued, Plaintiff and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach. The risk of another such breach is real, immediate, and substantial. If another breach occurs, Plaintiff will not have

an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

126. The hardship to Plaintiff if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Among other things, if another massive data breach occurs, Plaintiff will likely be subjected to fraud, identify theft, and other harms described herein. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

127. Issuance of the requested injunction will not do a disservice to the public interest. To the contrary, such an injunction would benefit the public by encouraging Defendant to take necessary action to prevent another data breach, thus eliminating the additional injuries that would result to Plaintiff and the millions of individuals whose PII would be at risk of future unauthorized disclosures.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the other members of the Classes alleged herein, respectfully request that the Court enter judgment in their favor and against Defendant as follows:

A. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff(s) as the representatives for the Classes and counsel for Plaintiff(s) as Class Counsel;

B. For an order declaring the Defendant's conduct violates the statutes and causes of action referenced herein;

C. For an order finding in favor of Plaintiff and the Classes on all counts asserted herein;

D. Ordering Defendant to pay for lifetime credit monitoring services for Plaintiff and the Classes;

E. For compensatory, statutory, and punitive damages in amounts to be determined by the Court and/or jury;

F. For prejudgment interest on all amounts awarded;

G. For an order of restitution and all other forms of equitable monetary relief;

H. For injunctive relief as pleaded or as the Court may deem proper; and

I. For an order awarding Plaintiff and the Classes their reasonable attorneys' fees and expenses and costs of suit, and any other expense, including expert witness fees; and

J. Such other relief as this Court deems just and proper.

DEMAND FOR JURY TRIAL

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiff demands a trial by jury of all claims in this Complaint and of all issues in this action so triable as of right.

Dated: July 1, 2024

Respectfully submitted,

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

Paul J. Doolittle
POULIN | WILLEY | ANASTOPOULO
32 Ann Street
Charleston, SC 29403
Telephone: (803) 222-2222
Fax: (843) 494-5536
Email: paul.doolittle@poulinwilley.com

Attorneys for Plaintiffs

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

CHRISTOPHER MILLER, individually and on behalf all others similarly situated

(b) County of Residence of First Listed Plaintiff Los Angeles County
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Joe Kendall, Kendall Law Group, PLLC, 3811 Turtle Creek Blvd., Suite 825, Dallas, TX 75219, 214/744-3000

DEFENDANTS

FRONTIER COMMUNICATIONS PARENT, INC.

County of Residence of First Listed Defendant
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ❒ 1 U.S. Government Plaintiff
- ❒ 3 Federal Question *(U.S. Government Not a Party)*
- ❒ 2 U.S. Government Defendant
- ☒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*
(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	❒ 1	❒ 1	Incorporated *or* Principal Place of Business In This State	❒ 4	☒ 4
Citizen of Another State	☒ 2	❒ 2	Incorporated *and* Principal Place of Business In Another State	❒ 5	❒ 5
Citizen or Subject of a Foreign Country	❒ 3	❒ 3	Foreign Nation	❒ 6	❒ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for: Nature of Suit Code Descriptions.

CONTRACT
- ❒ 110 Insurance
- ❒ 120 Marine
- ❒ 130 Miller Act
- ❒ 140 Negotiable Instrument
- ❒ 150 Recovery of Overpayment & Enforcement of Judgment
- ❒ 151 Medicare Act
- ❒ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ❒ 153 Recovery of Overpayment of Veteran's Benefits
- ❒ 160 Stockholders' Suits
- ☒ 190 Other Contract
- ❒ 195 Contract Product Liability
- ❒ 196 Franchise

REAL PROPERTY
- ❒ 210 Land Condemnation
- ❒ 220 Foreclosure
- ❒ 230 Rent Lease & Ejectment
- ❒ 240 Torts to Land
- ❒ 245 Tort Product Liability
- ❒ 290 All Other Real Property

TORTS

PERSONAL INJURY
- ❒ 310 Airplane
- ❒ 315 Airplane Product Liability
- ❒ 320 Assault, Libel & Slander
- ❒ 330 Federal Employers' Liability
- ❒ 340 Marine
- ❒ 345 Marine Product Liability
- ❒ 350 Motor Vehicle
- ❒ 355 Motor Vehicle Product Liability
- ❒ 360 Other Personal Injury
- ❒ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ❒ 365 Personal Injury - Product Liability
- ❒ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ❒ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ❒ 370 Other Fraud
- ❒ 371 Truth in Lending
- ❒ 380 Other Personal Property Damage
- ❒ 385 Property Damage Product Liability

CIVIL RIGHTS
- ❒ 440 Other Civil Rights
- ❒ 441 Voting
- ❒ 442 Employment
- ❒ 443 Housing/ Accommodations
- ❒ 445 Amer. w/Disabilities - Employment
- ❒ 446 Amer. w/Disabilities - Other
- ❒ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ❒ 463 Alien Detainee
- ❒ 510 Motions to Vacate Sentence
- ❒ 530 General
- ❒ 535 Death Penalty

Other:
- ❒ 540 Mandamus & Other
- ❒ 550 Civil Rights
- ❒ 555 Prison Condition
- ❒ 560 Civil Detainee - Conditions of Confinement

FORFEITURE/PENALTY
- ❒ 625 Drug Related Seizure of Property 21 USC 881
- ❒ 690 Other

LABOR
- ❒ 710 Fair Labor Standards Act
- ❒ 720 Labor/Management Relations
- ❒ 740 Railway Labor Act
- ❒ 751 Family and Medical Leave Act
- ❒ 790 Other Labor Litigation
- ❒ 791 Employee Retirement Income Security Act

IMMIGRATION
- ❒ 462 Naturalization Application
- ❒ 465 Other Immigration Actions

BANKRUPTCY
- ❒ 422 Appeal 28 USC 158
- ❒ 423 Withdrawal 28 USC 157

PROPERTY RIGHTS
- ❒ 820 Copyrights
- ❒ 830 Patent
- ❒ 835 Patent - Abbreviated New Drug Application
- ❒ 840 Trademark

SOCIAL SECURITY
- ❒ 861 HIA (1395ff)
- ❒ 862 Black Lung (923)
- ❒ 863 DIWC/DIWW (405(g))
- ❒ 864 SSID Title XVI
- ❒ 865 RSI (405(g))

FEDERAL TAX SUITS
- ❒ 870 Taxes (U.S. Plaintiff or Defendant)
- ❒ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
- ❒ 375 False Claims Act
- ❒ 376 Qui Tam (31 USC 3729(a))
- ❒ 400 State Reapportionment
- ❒ 410 Antitrust
- ❒ 430 Banks and Banking
- ❒ 450 Commerce
- ❒ 460 Deportation
- ❒ 470 Racketeer Influenced and Corrupt Organizations
- ❒ 480 Consumer Credit
- ❒ 490 Cable/Sat TV
- ❒ 850 Securities/Commodities/ Exchange
- ❒ 890 Other Statutory Actions
- ❒ 891 Agricultural Acts
- ❒ 893 Environmental Matters
- ❒ 895 Freedom of Information Act
- ❒ 896 Arbitration
- ❒ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ❒ 950 Constitutionality of State Statutes

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding | ❒ 2 Removed from State Court | ❒ 3 Remanded from Appellate Court | ❒ 4 Reinstated or Reopened | ❒ 5 Transferred from Another District *(specify)* | ❒ 6 Multidistrict Litigation - Transfer | ❒ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
28 U.S.C. § 1332(d)

Brief description of cause:
Data Breach

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.

DEMAND $

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ❒ No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE SEE ATTACHMENT DOCKET NUMBER

DATE 07/01/2024

SIGNATURE OF ATTORNEY OF RECORD /s/ Joe Kendall

FOR OFFICE USE ONLY

RECEIPT # AMOUNT APPLYING IFP JUDGE MAG. JUDGE