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

MARCELO MUTO, individually and on behalf of all others similarly situated, Plaintiff, v. FRONTIER COMMUNICATIONS PARENT, INC. Defendant.	Case No. 3:24-cv-01507 **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Marcelo Muto ("Plaintiff") individually and on behalf of all others similarly situated, by and through his undersigned counsel, brings this Class Action Complaint against Frontier Communications Parent, Inc. ("Frontier"). Plaintiff alleges the following upon information and belief based on and the investigation of counsel, except as to those allegations that specifically pertain to Plaintiff, which is alleged upon personal knowledge.

INTRODUCTION

1. Plaintiff and the proposed Class Members bring this class action lawsuit on behalf of all persons who entrusted Frontier with sensitive personally identifiable information ("PII")[1] that was subsequently exposed in a data breach, which Frontier publicly disclosed on June 6, 2024 (the "Data Breach" or the "Breach").

2. Plaintiff's claims arise from Defendant's failure to properly secure and safeguard PII that was entrusted to it, and its accompanying responsibility to store and transfer that information. More than 750,000 consumers were affected by the Data Breach, in which sensitive

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual.

personal information, including names, dates of birth, and Social Security numbers, were accessed by an unauthorized third party.[2]

3. Frontier is a telecommunications company headquartered in Dallas, Texas.[3] Frontier provides broadband internet services, digital television services, and computer technical support services to customers across 25 states.[4]

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

5. On or around April 14, 2024, Frontier detected unauthorized activity within its IT network.[5] On June 6, 2024, Frontier filed its first public notice of data breach and began sending out notice letters to anyone who was affected by Data Breach.[6]

6. Plaintiff's claims arise from Defendant's failure to safeguard PII provided by, and belonging to, its customers and failure to provide timely notice of the Data Breach.

7. Defendant failed to take precautions designed to keep its customers' PII secure.

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

---

[2] *Data Breach Notification: Frontier Communications Parent, Inc.,* OFFICE OF THE MAINE ATTORNEY GENERAL (June 6, 2024) https://apps.web.maine.gov/online/aeviewer/ME/40/8391c11f-2946-414a-bdc1-6ceff4ae0caa.shtml (last visited June 17, 2024).
[3] https://frontier.com (last visited June 15, 2024)
[4] *Id.*
[5] *Data Breach Notification: Fronter Communications Parent, Inc.,* OFFICE OF THE MAINE ATTORNEY GENERAL (June 6, 2024) https://apps.web.maine.gov/online/aeviewer/ME/40/8391c11f-2946-414a-bdc1-6ceff4ae0caa/6ea4c515-a3eb-4f11-955c-a714a320b142/document.html (last visited June 17, 2024).
[6] *Id.*

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

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

11. Defendant, despite having the financial wherewithal and personnel necessary to prevent the Data Breach, nevertheless failed to use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it maintained for Plaintiff and Class Members, causing the exposure of PII for Plaintiff and Class Members.

12. As a result of the Defendant's inadequate digital security and notice process, Plaintiff and Class Members' PII was exposed to criminals. Plaintiff and the Class have suffered and will continue to suffer injuries including financial losses caused by misuse of PII; the loss or diminished value of their PII as a result of the Data Breach; uncompensated lost time associated with detecting and preventing identity theft; and theft of personal and financial information.

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

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

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

PARTIES

Plaintiff

16. Plaintiff Marcelo Muto is a citizen of California and resides in Indio, California. Plaintiff Muto received a notice letter from Frontier dated June 6, 2024, informing him that his information was compromised in the Data Breach. As a consequence of the Data Breach, Plaintiff Muto has been forced to, and will continue to, invest significant time monitoring his accounts to detect and reduce the consequences of identity fraud. As a result of the Data Breach, plaintiff Muto is now subject to substantial and imminent risk of future harm. Plaintiff Muto would not have used Frontier's services had he known that it would expose his sensitive PII.

Defendant

17. Defendant Frontier is a telecommunications company incorporated in Delaware with its principal place of business located at 1919 McKinney Avenue, Dallas, Texas 75201. Defendant is a citizen of Texas. 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

18. 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 Defendant, and there are more than 100 putative Class Members. Plaintiff is a citizen of California. Defendant is a citizen of Texas.

19. This Court has personal jurisdiction over Defendant because Defendant is registered to do business and maintains its principal place of business in the Dallas Division of the Northern District of Texas.

20. Venue is proper in these District under 28 U.S.C. § 1391(b)(2) because Defendant is headquartered in the Dallas Division of the Northern District of Texas, and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

FACTUAL ALLEGATIONS

A. Background on Defendant

21. Defendant is a telecommunications company headquartered in Dallas, Texas.[7] Frontier provides broadband internet services, digital television services, and computer technical support services to customers across 25 states.[8]

22. In the ordinary course of its business practices, Defendant stores, maintains, and uses an individuals' PII, which includes Plaintiff and Class Members, including but not limited to information such as: full names; dates of birth; Social Security numbers; and account numbers.

[7] https://frontier.com (last visited June 17, 2024)
[8] *Id.*

23. Upon information and belief, Defendant made promises and representations to its customers, including Plaintiff and Class Members, that the PII collected from them would be kept safe, confidential, that the privacy of that information would be maintained.

24. Plaintiff and Class Members provided their PII to Defendant with the reasonable expectation and on the mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

25. As a result of collecting and storing the PII of Plaintiff and Class Members for its own financial benefit, Defendant had a continuous duty to adopt and employ reasonable measures to protect Plaintiff and the Class Members' PII from disclosure to third parties.

B. The Data Breach

26. On or around April 14, 2024, Frontier detected unusual activity within its computer network.[9] In response, Frontier secured its systems and then launched an investigation with the help of third-party data security experts.[10]

27. Frontier's investigation determined that an unauthorized actor may have obtained consumers sensitive PII including names, date of birth, and Social Security numbers.[11] Frontier first publicly disclosed the Data Breach on June 6, 2024 when it filed a notice of data breach with the Office of the Maine Attorney General[12] and began sending out notices to affected consumers

[9] *Data Breach Notification: Frontier Communications Parent, Inc.,* OFFICE OF THE MAINE ATTORNEY GENERAL (June 6, 2024) https://apps.web.maine.gov/online/aeviewer/ME/40/8391c11f-2946-414a-bdc1-6ceff4ae0caa.shtml (last visited June 17, 2024).
[10] George Fizmaurice, *Frontier Communications confirms over 750,000 people affected by data breach,* ITPoro (June 10, 2024), https://www.itpro.com/security/data-breaches/frontier-communications-confirms-over-750000-people-affected-in-data-breach (last visited June 17, 2024).
[11] Bill Toulas, *Frontier warns 750,000 of a data breach after extortion threats*, BleepingComputer (June 7, 2024) https://www.bleepingcomputer.com/news/security/frontier-warns-750-000-of-a-data-breach-after-extortion-threats/ (last visited June 17, 2024).
[12] *Data Breach Notification: Frontier Communications Parent, Inc.,* OFFICE OF THE MAINE ATTORNEY GENERAL (June 6, 2024) https://apps.web.maine.gov/online/aeviewer/ME/40/8391c11f-2946-414a-bdc1-6ceff4ae0caa.shtml (last visited June 17, 2024).

that same day.[13]

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

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

C. Defendant's Failure to Prevent, Identify and Timely Report the Data Breach

30. Defendant admits that an unauthorized third party accessed its network systems in order to obtain sensitive information about its current and former customers.

31. Defendant failed to take adequate measures to protect its computer systems against unauthorized access.

32. Defendant was not only aware of the importance of protecting the PII that it maintains, as alleged, it promoted its capability to do so, as evident from its Privacy Policy.[14]

33. The PII that Defendant allowed to be exposed in the Data Breach is the type of private information that Defendant knew or should have known would be the target of cyberattacks.

34. Despite its own knowledge of the inherent risks of cyberattacks, and notwithstanding the FTC's data security principles and practices,[15] Defendant failed to disclose that its systems and security practices were inadequate to reasonably safeguard its past and present customers' sensitive personal information.

---

[13] *Id.*

[14] *Frontier Communications Privacy Policy, Frontier*, https://frontier.com/corporate/privacy-policy (last visited June 17, 2024).

[15] *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (Oct. 2016), https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last visited June 17, 2024).

35. The FTC directs businesses to use an intrusion detection system to expose a breach as soon as it occurs, monitor activity for attempted hacks, and have an immediate response plan if a breach occurs.[16] Immediate notification of a Data Breach is critical so that those impacted can take measures to protects themselves.

36. Despite this guidance, Defendant delayed the notification of the Data Breach. Based on Frontier's filing with the Office of the Maine Attorney General, the Data Breach is believed to have occurred on or around April 14, 2024, yet, by its own admission, Defendant did not begin informing impacted consumers until nearly two months later on June 6, 2024.

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

37. Victims of data breaches are susceptible to becoming victims of identity theft.

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

39. The type of data that was accessed and compromised here – such as full names and Social Security numbers – can be used to perpetrate fraud and identity theft. Social Security numbers are widely regarded as the most sensitive information hackers can access. Social Security numbers and dates of birth together constitute high risk data.

40. Plaintiff and Class members face a substantial risk of identity theft given that their Social Security numbers, addresses, dates of birth, and other important PII were compromised in

[16] *Id.*
[17] *Prevention and Preparedness*, NEW YORK STATE POLICE, https://troopers.ny.gov/prevention-and-preparedness (last visited June 17, 2024).

the Data Breach. Once a Social Security number is stolen, it can be used to identify victims and target them in fraudulent schemes and identity theft.

41. Stolen PII is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines. Law enforcement has difficulty policing the "dark web" due to this encryption, which allows users and criminals to conceal their identities and online activity.

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

43. For example, in one recent case unsealed by the U.S. Department of Justice, an Illinois man led a group of criminals in marketing almost 50,000 stolen payment cards on dark web marketplaces, generating at least $1 million in cryptocurrency.[19]

44. PII remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, someone can purchase a full range of documents that will allow identity theft, including $500 for a high-quality U.S. driver's license, $25 for a hacked social media account, $110 for credit card information, and $150 for banking account information.[20]

45. A compromised or stolen Social Security number cannot be addressed as simply as a stolen credit card. An individual cannot obtain a new Social Security number without significant

---

[18] *Shining a Light on the Dark Web with Identity Monitoring*, IDENTITYFORCE (Dec. 28, 2020) https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring (last visited June 17, 2024).

[19] *Is Your Information for Sale on the Dark Web?* (Feb. 26 ,2024) https://verafin.com/2024/02/is-your-information-for-sale-on-the-dark-web/ (last visited June 17, 2024).

[20] *Revealed – how much is personal information worth on the dark web?* (May 1, 2023) https://www.insurancebusinessmag.com/us/news/breaking-news/revealed--how-much-is-personal-information-worth-on-the-dark-web-444453.aspx (last visited June 17, 2024).

work. Preventive action to defend against the possibility of misuse of a Social Security number is not permitted; rather, an individual must show evidence of actual, ongoing fraud activity to obtain a new number. Even then, however, obtaining a new Social Security number may not suffice. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[21]

46. The PII compromised in the Data Breach demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained: "[c]ompared to credit card information, personally identifiable information and Social Security numbers are worth more than 10 times on the black market."[22]

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

48. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[24] Defendant did not rapidly report to Plaintiff and Class Members that their PII had been stolen.

49. As a result of the Data Breach, the PII of Plaintiff and Class Members have been exposed to criminals for misuse. The injuries suffered by Plaintiff and Class Members, or likely to be suffered thereby as a direct result of Defendant's Data Breach, include: (a) theft of their PII; (b)

---

[21] *Id*.
[22] *Experts advise compliance not same as security*, RELIAS MEDIA (Mar. 1, 2015) https://www.reliasmedia.com/articles/134827-experts-advise-compliance-not-same-as-security (last visited June 17, 2024).
[23] *2019 Internet Crime Report Released*, FBI, https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120#:~:text=IC3%20received%20467%2C361%20complaints%20in,%2Ddelivery%20scams%2C%20and%20extortion. (last visited June 17, 2024).
[24] *Id.*

costs associated with the detection and prevention of identity theft; (c) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the consequences of this breach; (d) invasion of privacy; (e) the emotional distress, stress, nuisance, and annoyance of responding to, and resulting from, the Data Breach; (f) the actual and/or imminent injury arising from actual and/or potential fraud and identity theft resulting from their personal data being placed in the hands of the ill-intentioned hackers and/or criminals; (g) damage to and diminution in value of their personal data entrusted to Defendant with the mutual understanding that Defendant would safeguard their PII against theft and not allow access to and misuse of their personal data by any unauthorized third party; and (h) the continued risk to their PII, which remains in the possession of Defendant, and which is subject to further injurious breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff and Class Members' PII.

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

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

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

CLASS ALLEGATIONS

53. Plaintiff brings this action pursuant to Rule 23 of the Federal Rules of Civil Procedure, individually and on behalf of the following Nationwide Class:

> All persons in the United States whose personal information was compromised in the Data Breach publicly announced by Defendant in June of 2024 (the "Class").

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

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

56. This action may be certified as a class action under Federal Rule of Civil Procedure 23 because it satisfies the numerosity, commonality, typicality, adequacy, and superiority requirements therein.

57. Numerosity (Rule 23(a)(1)): The Class is so numerous that joinder of all Class Members is impracticable. Although the precise number of such persons is unknown, and the facts are presently within the sole knowledge of Defendant, Plaintiff estimates that the Class is comprised of hundreds of thousands of Class Members. The Class is sufficiently numerous to warrant certification.

58. Typicality of Claims (Rule 23(a)(3)): Plaintiff's claims are typical of those of other Class Members because, Plaintiff, like the Class Members, had his PII compromised as a result of the Data Breach. Plaintiff is a member of the Class, and his claims are typical of the claims of the members of the Class. The harm suffered by Plaintiff is similar to that suffered by all other Class Members that was caused by the same misconduct by Defendant.

59. Adequacy of Representation (Rule 23(a)(4)): Plaintiff will fairly and adequately represent and protect the interests of the Class. Plaintiff has no interests antagonistic to, nor in conflict with, the Class. Plaintiff has retained competent counsel who are experienced in consumer and commercial class action litigation and who will prosecute this action vigorously.

60. Superiority (Rule 23(b)(3)): A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Because the monetary damages suffered by individual Class Members is relatively small, the expense and burden of individual litigation make it impossible for individual Class Members to seek redress for the wrongful conduct asserted herein. If Class treatment of these claims is not available, Defendant will likely continue its wrongful conduct, will unjustly retain improperly obtained revenues, or will otherwise escape

liability for its wrongdoing as asserted herein.

61. Predominant Common Questions (Rule 23(a)(2)): The claims of all Class Members present common questions of law or fact, which predominate over any questions affecting only individual Class Members, including:

a. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

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

c. Whether Defendant's storage of Class Member's PII was done in a negligent manner;

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

e. Whether Defendant's conduct was negligent;

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

g. Whether Defendant took sufficient steps to secure its customers' PII;

h. Whether Defendant was unjustly enriched;

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

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

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

64. The prosecution of separate actions by individual members of the Class would run the risk of inconsistent or varying adjudications and establish incompatible standards of conduct for Defendant. Prosecution as a class action will eliminate the possibility of repetitious and inefficient litigation.

65. Defendant has acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive relief or corresponding declaratory relief with respect to the Class as a whole.

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

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and All Class Members)

67. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above in paragraphs 1 through 15 and paragraphs 21 through 52 as though fully set forth herein.

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

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

70. Defendant had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiff and Class Members' PII.

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

72. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards, applicable standards of care from statutory authority like Section 5 of the FTC Act, and other requirements discussed herein, and to ensure that its

systems and networks, and the personnel responsible for them, adequately protected its customers' PII.

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

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

75. Defendant breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff and Class Members' PII.

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

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

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

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

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

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

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

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

81. It was foreseeable that Defendant's failure to use reasonable measures to protect Plaintiff and Class Members' PII would result in injury to Plaintiff and Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches.

82. It was foreseeable that the failure to adequately safeguard Plaintiff and Class Members' PII would result in injuries to Plaintiff and Class Members.

83. Defendant's breach of duties owed to Plaintiff and Class Members caused Plaintiff and Class Members' PII to be compromised.

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

85. As a result of Defendant's failure to timely notify Plaintiff and Class Members that their PII had been compromised, Plaintiff and Class Members are unable to take the necessary precautions to mitigate damages by preventing future fraud.

86. As a result of Defendant's negligence and breach of duties, Plaintiff and Class Members are in danger of imminent harm in that their PII, which is still in the possession of third parties, will be used for fraudulent purposes, and Plaintiff and Class Members have and will suffer damages including: a substantial increase in the likelihood of identity theft; the compromise, publication, and theft of their personal information; loss of time and costs associated with the prevention, detection, and recovery from unauthorized use of their personal information; the continued risk to their personal information; future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the personal information compromised as a result of the Data Breach; and overpayment for the services or products that were received without adequate data security.

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

87. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above in paragraphs 1 through 15 and paragraphs 21 through 52 as though fully set forth herein.

88. 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 T-Mobile of failing to use reasonable measures to protect Plaintiff and Class members' Private Information. Various FTC publications and orders also form the basis of Defendant's duty.

89. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiff's and Class members' Private Information and not complying with industry standards.

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

91. Defendant violation of Section 5 of the FTC Act constitutes negligence per se.

92. Class members are consumers within the class of persons Section 5 of the FTC Act were intended to protect.

93. Moreover, the harm that has occurred is the type of harm the FTC Act was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class members.

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

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

95. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above in paragraphs 1 through 15 and paragraphs 21 through 52 as though fully set forth herein.

96. Plaintiff and Class members, upon information and belief, entered into express contracts with Defendant that included Defendant's promise to protect nonpublic personal information given to Defendant or that Defendant gathered on its own, from disclosure.

97. Plaintiff and Class members performed their obligations under the contracts when they provided their PII to Defendant for services and when they paid for the service provided by Defendant.

98. Defendant breached its contractual obligations to protect the nonpublic personal information Defendant possessed and was entrusted with when the information was accessed by unauthorized persons as part of the data breach.

99. As a direct and proximate result of Defendant's above-described breach of contract, Plaintiff and Class members have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

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

100. Plaintiff incorporates by reference and re-allege each and every allegation set forth above in paragraphs 1 through 15 and paragraphs 21 through 52 as though fully set forth herein.

101. Plaintiff and the Class provided and entrusted their PII to Defendant. Plaintiff and the Class provided their PII to Defendant as part of Defendant's regular business practices.

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

103. Pursuant to these implied contracts, Plaintiff and Class Members provided Defendant with their PII in order for Defendant to provide services, for which Defendant is compensated. In exchange, Defendant agreed to, among other things, and Plaintiff and the Class understood that Defendant would: (1) provide services to Plaintiff and Class Members; (2) take reasonable measures to protect the security and confidentiality of Plaintiff and Class Members' PII; and (3) protect Plaintiff and Class Members' PII in compliance with federal and state laws and regulations and industry standards.

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

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

106. Indeed, implicit in the agreement between Defendant and its customers was the obligation that both parties would maintain information confidentially and securely.

107. These exchanges constituted an agreement and meeting of the minds between the parties: Plaintiff and Class Members would provide their PII in exchange for services by

Defendant. These agreements were made by Plaintiff and Class Members as Defendant's customers.

108. When the parties entered into an agreement, mutual assent occurred. Plaintiff and Class Members would not have disclosed their PII to Defendant but for the prospect of utilizing Defendant's services. Conversely, Defendant presumably would not have taken Plaintiff and Class Members' PII if it did not intend to provide Plaintiff and Class Members with its services.

109. Defendant was therefore required to reasonably safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure and/or use.

110. Plaintiff and Class Members accepted Defendant's offer of services and fully performed their obligations under the implied contract with Defendant by providing their PII, directly or indirectly, to Defendant, among other obligations.

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

112. Defendant breached the implied contracts with Plaintiff and Class Members by failing to reasonably safeguard and protect Plaintiff and Class Members' PII.

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

114. Instead of spending adequate financial resources to safeguard Plaintiff and Class Members' PII, which Plaintiff and Class Members were required to provide to Defendant, Defendant instead used that money for other purposes, thereby breaching their implied contracts it had with Plaintiff and Class Members.

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

COUNT V
UNJUST ENRICHMENT
(On behalf of Plaintiff and All Class Members)

116. Plaintiff incorporates by reference and re-allege each and every allegation set forth above in paragraphs 1 through 15 and paragraphs 21 through 52 as though fully set forth herein.

117. Plaintiff and Class Members conferred a benefit upon Defendant by using Defendant's services.

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

119. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff and the Class Members' services and their PII because Defendant failed to adequately protect their PII. Plaintiff and the proposed Class would not have provided their PII to Defendant or utilized their services had they known Defendant would not adequately protect their PII.

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

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, seeks judgment against Defendant, as follows:

(a) For an order determining that this action is properly brought as a class action and certifying Plaintiff as the representatives of the Class and his counsel as Class Counsel;

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

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

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

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

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

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

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

JURY TRIAL DEMANDED

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

Dated: June 17, 2024

Respectfully submitted,

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

Courtney E. Maccarone*
LEVI & KORSINSKY, LLP
33 Whitehall Street, 17th Floor
New York, NY 10004
Telephone: (212) 363-7500
Facsimile: (212) 363-7171
Email: cmaccarone@zlk.com

**pro hac vice* forthcoming

Counsel for Plaintiff

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

MARCELO MUTO, individually and on behalf all others similarly situated

(b) County of Residence of First Listed Plaintiff Riverside 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	TORTS		FORFEITURE/PENALTY	BANKRUPTCY	OTHER STATUTES
❒ 110 Insurance	PERSONAL INJURY	PERSONAL INJURY	❒ 625 Drug Related Seizure of Property 21 USC 881	❒ 422 Appeal 28 USC 158	❒ 375 False Claims Act
❒ 120 Marine	❒ 310 Airplane	❒ 365 Personal Injury - Product Liability	❒ 690 Other	❒ 423 Withdrawal 28 USC 157	❒ 376 Qui Tam (31 USC 3729(a))
❒ 130 Miller Act	❒ 315 Airplane Product Liability	❒ 367 Health Care/ Pharmaceutical Personal Injury Product Liability		PROPERTY RIGHTS	❒ 400 State Reapportionment
❒ 140 Negotiable Instrument	❒ 320 Assault, Libel & Slander	❒ 368 Asbestos Personal Injury Product Liability		❒ 820 Copyrights	❒ 410 Antitrust
❒ 150 Recovery of Overpayment & Enforcement of Judgment	❒ 330 Federal Employers' Liability	PERSONAL PROPERTY	LABOR	❒ 830 Patent	❒ 430 Banks and Banking
❒ 151 Medicare Act	❒ 340 Marine	❒ 370 Other Fraud	❒ 710 Fair Labor Standards Act	❒ 835 Patent - Abbreviated New Drug Application	❒ 450 Commerce
❒ 152 Recovery of Defaulted Student Loans (Excludes Veterans)	❒ 345 Marine Product Liability	❒ 371 Truth in Lending	❒ 720 Labor/Management Relations	❒ 840 Trademark	❒ 460 Deportation
❒ 153 Recovery of Overpayment of Veteran's Benefits	❒ 350 Motor Vehicle	❒ 380 Other Personal Property Damage	❒ 740 Railway Labor Act	SOCIAL SECURITY	❒ 470 Racketeer Influenced and Corrupt Organizations
❒ 160 Stockholders' Suits	❒ 355 Motor Vehicle Product Liability	❒ 385 Property Damage Product Liability	❒ 751 Family and Medical Leave Act	❒ 861 HIA (1395ff)	❒ 480 Consumer Credit
☒ 190 Other Contract	❒ 360 Other Personal Injury		❒ 790 Other Labor Litigation	❒ 862 Black Lung (923)	❒ 490 Cable/Sat TV
❒ 195 Contract Product Liability	❒ 362 Personal Injury - Medical Malpractice		❒ 791 Employee Retirement Income Security Act	❒ 863 DIWC/DIWW (405(g))	❒ 850 Securities/Commodities/ Exchange
❒ 196 Franchise				❒ 864 SSID Title XVI	❒ 890 Other Statutory Actions
				❒ 865 RSI (405(g))	❒ 891 Agricultural Acts
					❒ 893 Environmental Matters
					❒ 895 Freedom of Information Act
REAL PROPERTY	CIVIL RIGHTS	PRISONER PETITIONS	IMMIGRATION	FEDERAL TAX SUITS	❒ 896 Arbitration
❒ 210 Land Condemnation	❒ 440 Other Civil Rights	Habeas Corpus:	❒ 462 Naturalization Application	❒ 870 Taxes (U.S. Plaintiff or Defendant)	❒ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
❒ 220 Foreclosure	❒ 441 Voting	❒ 463 Alien Detainee	❒ 465 Other Immigration Actions	❒ 871 IRS—Third Party 26 USC 7609	❒ 950 Constitutionality of State Statutes
❒ 230 Rent Lease & Ejectment	❒ 442 Employment	❒ 510 Motions to Vacate Sentence			
❒ 240 Torts to Land	❒ 443 Housing/ Accommodations	❒ 530 General			
❒ 245 Tort Product Liability	❒ 445 Amer. w/Disabilities - Employment	❒ 535 Death Penalty			
❒ 290 All Other Real Property	❒ 446 Amer. w/Disabilities - Other	Other:			
	❒ 448 Education	❒ 540 Mandamus & Other			
		❒ 550 Civil Rights			
		❒ 555 Prison Condition			
		❒ 560 Civil Detainee - Conditions of Confinement			

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 06/17/2024

SIGNATURE OF ATTORNEY OF RECORD /s/ Joe Kendall

FOR OFFICE USE ONLY

RECEIPT # AMOUNT APPLYING IFP JUDGE MAG. JUDGE