UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

AMBER WILSON, *individually and on behalf of all others similarly situated*, Plaintiff, v. FRONTIER COMMUNICATIONS PARENT, INC., Frontier.	Civil Action No. 3:24-CV-1418-L Consolidated with Civil Action Nos. 3:24-cv-01421; 3:24-cv-01423; 3:24-cv-01429; 3:24-cv-01435; 3:24-cv-01441; 3:24-cv-01444; 3:24-cv-01468; 3:24-cv-01492; 3:24-cv-01497; 3:24-cv-01501; 3:24-cv-01507; 3:24-cv-01516; 3:24-cv-01517; 3:24-cv-01589; 3:24-cv-01592; 3:24-cv-01671. **JURY TRIAL DEMANDED**

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Brian Carolus, Adrian Graham, Christopher Miller, Lauren Morgan, Marcelo Muto, Ian Terrell, Richard Retter, Joselyn Chiong, Timothy Morgan, James Pratt II, Seth Burton, Lori Rusk, and Gerald Wilson ("Plaintiffs"), individually and on behalf of all others similarly situated ("Class Members"), bring this action against Defendant Frontier Communications Parent, Inc. ("Frontier"), alleging as follows upon Plaintiffs' personal knowledge, information and belief, and investigation of counsel.

I. INTRODUCTION

1. This action arises from Frontier's failure to properly secure and safeguard Plaintiffs' and approximately 750,000 Class Members' sensitive personal identifying information[1] ("PII"),

[1] The Federal Trade Commission ("FTC") defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth. . . .." 17 C.F.R. § 248.201(b)(8).

which as a result, is now in a notorious criminal ransomware group's possession and published on the dark web.

2. Due to Frontier's deficient data security, the notorious cybercriminal organization known as RansomHub accessed Frontier's network servers and systems and exfiltrated Plaintiffs' and Class Members' PII stored therein, including their names, dates of birth, Social Security numbers, usage data, and other sensitive and confidential information (collectively, "Private Information"), causing widespread injuries and damages to Plaintiffs and Class Members (the "Data Breach").

3. According to its website, Frontier is the largest pure-play fiber internet provider in the United States, serving around 4.5 million customers across the country and generating billions of dollars in annual revenue.[2]

4. Plaintiffs and Class Members are current and former customers of Frontier who, as a condition and in exchange for receiving residential internet and/or television services from Frontier, were required to and did entrust Frontier with their confidential, non-public Private Information. Frontier collected, used, and maintained Plaintiffs' and Class Members' Private Information to facilitate its operations, including providing and billing for its services, and stored and transmitted this Private Information on its network servers and systems.

5. Businesses that handle customers' Private Information like Frontier owe the individuals to whom that information relates a duty to adopt reasonable measures to protect it from disclosure to unauthorized third parties, and to keep it safe and confidential. This duty arises under contract, statutory and common law, federal and state law and regulation, industry standards, and

[2] *See About Frontier*, Frontier Communications Parent, Inc. (2024), https://newsroom.frontier.com/about-frontier/ (last visited Sept. 4, 2024).

representations made to Plaintiffs and Class Members, and because it is foreseeable that the exposure of Private Information to unauthorized persons—especially hackers with nefarious intentions—will harm the affected individuals, including but not limited to the invasion of their private financial matters.

6. Frontier breached its duties owed to Plaintiffs and Class Members by failing to safeguard the Private Information it collected from them and maintained, including by failing to implement industry standards for data security to protect the sensitive data against cyberattacks, which allowed the RansomHub cybergang to access and exfiltrate nearly one million individuals' Private Information from Frontier's care.

7. According to Frontier's form notice to consumers about the Data Breach,[3] on April 14, 2024, Frontier "detected unauthorized access to some of [its] internal IT systems," and ultimately determined that its current and former customers' Private Information, including their names, dates of birth, and Social Security Numbers, had been compromised and disclosed.

8. Plaintiffs have now learned that RansomHub was behind the Data Breach and has published Plaintiffs' and Class Members' stolen Private Information to its dark web leak site, where, as of September 4, 2024, it had already been viewed over 34,000 times.

9. Upon information and belief, the mechanism of the RansomHub cyberattack and potential for improper disclosure of Plaintiffs' and Class Members' Private Information was a known risk to Frontier, and thus, Frontier knew failing to take reasonable steps to secure the Private Information left it in a dangerous condition.

10. Despite knowing the risks, Frontier failed to adequately protect Plaintiffs' and

[3] Available at https://ago.vermont.gov/sites/ago/files/documents/2024-06-06%20Frontier%20Communications%20Parent%20Data%20Breach%20Notice%20to%20Consumers.pdf (last visited Sept. 4, 2024).

Class Members' Private Information—and failed to even encrypt or redact this highly sensitive data. This unencrypted, unredacted Private Information was compromised due to Frontier's negligent and/or careless acts and omissions and its utter failure to protect Plaintiffs' and Class Members' sensitive data.

11. Frontier breached its duties and obligations by failing in one or more of the following ways: (a) to design, implement, monitor, and maintain reasonable network safeguards against foreseeable threats; (b) to design, implement, and maintain reasonable data retention policies; (c) to adequately train or oversee staff and service providers regarding data security; (d) to comply with industry-standard data security practices; (e) to warn Plaintiffs and Class Members of Frontier's inadequate data security practices; (f) to encrypt or adequately encrypt the Private Information it collected and stored; (g) to recognize or detect that its network had been compromised and accessed in a timely manner to mitigate the harm; (h) to utilize widely available software able to detect and prevent this type of attack; and (i) to otherwise secure the Private Information using reasonable and effective data security procedures free of foreseeable vulnerabilities and breaches.

12. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality and security of their Private Information. In providing their Private Information to Frontier, Plaintiffs and Class Members reasonably expected this sophisticated business entity to keep their Private Information confidential and security maintained, to use it only for business purposes, and to disclose it only as authorized. Frontier failed to do so, causing the unauthorized disclosure of Plaintiffs and Class Members' Private Information in the Data Breach.

13. RansomHub targeted and obtained Plaintiffs' and Class Members' Private Information from Frontier because of the data's value in exploiting and stealing Plaintiffs' and

Class Members' identities. As a direct and proximate result of Frontier's inadequate data security and breaches of duties to handle Private Information with reasonable care, Plaintiffs' and Class Members' Private Information was accessed by cybercriminals that have now disseminated it to at least 34,000 unknown actors through the RansomHub dark web leak site. The present and continuing risk to Plaintiffs and Class Members as victims of the Data Breach will remain for their respective lifetimes.

14. The harm resulting from a cyberattack like this Data Breach manifests in numerous ways including identity theft and financial fraud, and the exposure of an individual's Private Information due to breach ensures that he or she will be at a substantially increased and certainly impending risk of identity theft crimes compared to the rest of the population, potentially for the rest of his or her life. Mitigating that risk, to the extent even possible, requires individuals to devote significant time and money to closely monitor their credit, financial accounts, and email accounts, and take several additional prophylactic measures.

15. The risk of identity theft caused by this Data Breach is impending and has materialized, as Plaintiffs' and Class Members' Private Information was targeted, accessed, and misused by a notorious cybercriminal group that has already disseminated the Private Information to nefarious actors on the dark web.

16. As a result of Frontier's deficient cybersecurity and the consequential Data Breach, Plaintiffs and Class Members have suffered and will continue to suffer concrete injuries in fact including, *inter alia*, (a) actual and/or materialized and imminent risk of identity theft and fraud; (b) financial costs incurred due to actual identity theft; (c) lost time and productivity dealing with actual identity theft; (d) financial costs incurred mitigating the materialized risk and imminent threat of identity theft; (e) loss of time and loss of productivity incurred mitigating the materialized

risk and imminent threat of identity theft; (f) deprivation of value of their Private Information; (g) loss of privacy; (h) emotional distress including anxiety and stress in with dealing with the Data Breach; (i) loss of the benefit of their bargains with Frontier; and (j) the continued risk to their sensitive Private Information, which remains in Frontier's possession and subject to further breaches, so long as Frontier fails to undertake appropriate and adequate measures to protect the confidential data it collects and maintains.

17. To recover for these harms, Plaintiffs, individually and on behalf of the Classes as defined herein, bring claims for negligence/negligence *per se*, breach of contract, invasion of privacy/intrusion upon seclusion, state consumer protection laws, unjust enrichment, and declaratory relief, to address Frontier's inadequate safeguarding of Plaintiffs' and Class Members' sensitive Private Information.

18. Plaintiffs, individually and on behalf of putative Class Members, seek compensatory, consequential, nominal, statutory, and punitive damages, attorneys' fees and costs, declaratory judgment, and injunctive relief requiring Frontier to (a) disclose, expeditiously, the full nature of the Data Breach and the types of Private Information exposed; (b) implement improved data security practices to reasonably guard against future breaches of Private Information in Frontier's possession; and (c) provide, at Frontier's own expense, all impacted Data Breach victims with lifetime credit monitoring and identity theft protection services.

II. PARTIES

19. Plaintiff Brian Carolus is a citizen and resident of California.

20. Plaintiff Adrian Graham is a citizen and resident of California.

21. Plaintiff Christopher Miller is a citizen and resident of California.

22. Plaintiff Lauren Morgan is a citizen and resident of California.

23. Plaintiff Marcelo Muto is a citizen and resident of California.

24. Plaintiff Ian Terrell is a citizen and resident of California.

25. Plaintiff Richard Retter is a citizen and resident of Connecticut.

26. Plaintiff Joselyn Chiong is a citizen and resident of Florida.

27. Plaintiff Timothy Morgan is a citizen and resident of Florida.

28. Plaintiff James Pratt II is a citizen and resident of Illinois.

29. Plaintiff Seth Burton is a citizen and resident of New York.

30. Plaintiff Lori Rusk is a citizen and resident of Ohio.

31. Plaintiff Gerald Wilson is a citizen and resident of South Carolina.

32. Defendant Frontier Communications Parent, Inc. is Delaware corporation with its headquarters and principal place of business at 1919 McKinney Avenue, Dallas, Texas, 75201.

III. JURISDICTION AND VENUE

15. This Court has personal jurisdiction over Frontier because its principal place of business is in Texas, and because it engages in substantial and continuous activities and conduct business in this state.

16. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because the amount in controversy exceeds $5 million, exclusive of interest and costs, the number of Class Members is over 100, and at least one Class Member is a citizen of a state that is diverse from Frontier's citizenship, namely, all Plaintiffs. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

17. The Court has supplemental jurisdiction over Plaintiffs' claims arising under state law pursuant to 28 U.S.C. § 1367.

18. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because Frontier's

principal place of business is located in this District, and a substantial part of the events giving rise to this action and Plaintiffs' claims occurred in this District.

IV. FACTUAL ALLEGATIONS

A. Frontier Collects and Maintains Private Information and Promises to Protect It.

19. Frontier is the largest pure-play fiber internet provider in the United States, reporting $8.6 billion in revenue for the 2022 fiscal year and serving over 4.5 million customers across the United States.

20. To facilitate Frontier's operational and financial functions, including contracting with customers, furnishing its products and services, and billing customers, Frontier collects and maintains its customers' Private Information.

21. Plaintiffs and Class Members are current and former Frontier customers who, as a condition of and in exchange for receiving internet products and services from Frontier, were required to entrust Frontier with their sensitive Private Information including their names, dates of birth, Social Security numbers, financial account information, usage data, and other sensitive data.

22. Frontier derived economic benefits from collecting Plaintiffs' and Class Members' Private Information. Without the required submission of Private Information, Frontier could not perform its revenue-generating operations, including contracting with customers, furnishing its products and services, or billing for products and services provided.

23. At all relevant times, Frontier knew it was using its networks to store and transmit Plaintiffs' and Class Members' valuable, sensitive Private Information and that as a result, its systems would be attractive targets for cybercriminals.

24. Frontier also knew that any breach of its information technology network servers and systems and exposure of the data stored therein would result in the increased risk of identity

theft and fraud for the thousands of individuals whose Private Information was compromised, as well as intrusion into their private personal and financial matters.

25. In exchange for receiving Plaintiffs' and Class Members' Private Information, Frontier promised to safeguard the sensitive, confidential data and to only use it for authorized and legitimate purposes.

26. Frontier made promises and representations to its customers, including Plaintiffs and Class Members, that the Private Information it collected from them would be kept safe and confidential, the information's privacy would be maintained, and Frontier would delete any sensitive information after it was no longer required to maintain it.

27. Indeed, the Frontier Communications Privacy Policy in effect when the Data Breach occurred and published on Frontier's website at the time, promised and assured, "Protecting the privacy of our customers is important to Frontier."[4]

28. Frontier's Privacy Policy further promised and warranted to Frontier's customers, including Plaintiffs and Class Members, "We 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."[5]

29. Frontier's Privacy Policy additionally promised, "Personally identifiable and other sensitive records are retained only as long as reasonably necessary for business, accounting, tax, or legal purposes."[6]

30. Frontier's Privacy Policy also promised and assured customers that the Private Information Frontier collects from them will be used only for specific, enumerated purposes related

[4] Available https://web.archive.org/web/20240407052234/https://frontier.com/corporate/privacy-policy (last visited Sept. 4, 2024).
[5] *Id.*
[6] *Id.*

to Frontier's business or legal obligations—none of which permitted purposes include disclosure to a notorious cybercriminal group, as in this Data Breach.

31. Upon information and belief, Frontier's Privacy Policy is and was provided, and applicable, to all of Frontier's current and former residential internet, television, and landline customers, including Plaintiffs and Class Members, when they contracted with Frontier for home internet products and services.

32. Frontier's promises to adequately maintain and protect Plaintiffs' and Class Members' Private Information demonstrates its understanding that such data's confidentiality and integrity is critical.

33. Indeed, Frontier reiterates that understanding through a blog post titled *Should You Worry When There's a Data Breach?*, published to its website on March 20, 2024 (less than one month before the Data Breach occurred), which expressly advises consumers in part as follows:

> Companies will often store [Private Information], and **it's up to them to keep it secure from hackers**. But it doesn't always happen.
>
> In 2023, more than 353 million individuals had sensitive data accessed by an unauthorized threat actor. **The risk of your personal information getting exposed is serious**.
>
> **You don't have control over a company's cybersecurity**. But there are actions you can take to minimize the risk of your identity theft in the event of a data breach.
>
> * * *
>
> A data breach affects you in several ways. **It increases your chances of becoming a victim of identity or financial theft**. Hackers can use a leaked password to access other accounts that have the same password. It can take some effort to recover from getting hacked online.[7]

[7] Nguyen, S., *Should You Worry When There's a Data Breach?*, Frontier Communications Parent, Inc. (Mar. 20, 2024), https://blog.frontier.com/2024/03/should-you-worry-when-theres-a-data-breach/ (last visited Sept. 4, 2024) (emphasis added).

34. Consumers in general value the confidentiality of their Private Information and demand security to safeguard it. For their part, Plaintiffs and Class Members have taken reasonable steps to maintain their Private Information in confidence and privacy.

35. Plaintiffs and Class Members provided their Private Information to Frontier with the reasonable expectation and mutual understanding that Frontier would comply with its obligations to keep such information confidential and secure from unauthorized access.

36. Plaintiffs and Class Members relied on Frontier's sophistication to keep their Private Information confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information.

37. Plaintiffs and Class Members would not have entrusted their Private Information to Frontier in the absence of its promises to safeguard that information, including in the manners set forth in Frontier's Privacy Policy.

38. Frontier derived a substantial economic benefit from collecting Plaintiffs' and Class Members' Private Information. Without the required submission of Private Information, Frontier could not contract with customers, furnish its products and services, or bill customers.

39. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Frontier assumed legal and equitable duties to Plaintiffs and Class Members, and knew or should have known that it was responsible for protecting their Private Information from unauthorized disclosure. Frontier failed to do so, causing this Data Breach.

B. Frontier Failed to Adequately Safeguard Plaintiffs' and Class Members' Private Information, causing the Data Breach.

40. Frontier collected and maintained its current and former customers' Private Information on its computer information technology systems and networks, including when the Data Breach occurred.

41. The information held by Frontier at the time of the Data Breach included the unencrypted Private Information of Plaintiffs and Class Members.

42. On or about June 6, 2024, Frontier began sending Plaintiffs and other Data Breach victims letters titled *Notice of Data Breach* ("Notice Letters").

43. The Notice Letters generally inform as follows, in part:

> We are writing to inform you that some of your personal information may have been accessed by a third party during a recent cyber incident at Frontier Communications Parent, Inc. ("Frontier").
>
> * * *
>
> **What happened?**
> On April 14, 2024, we detected unauthorized access to some of our internal IT systems. Our investigation identified your personal information among the data affected by this incident.
>
> **What personal information was involved?**
> The personal information involved includes your name, Date of Birth, and Social Security number.

44. Omitted from the Notice Letters are crucial details like the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiffs and Class Members, who retain a vested interest in ensuring that their Private Information is protected.

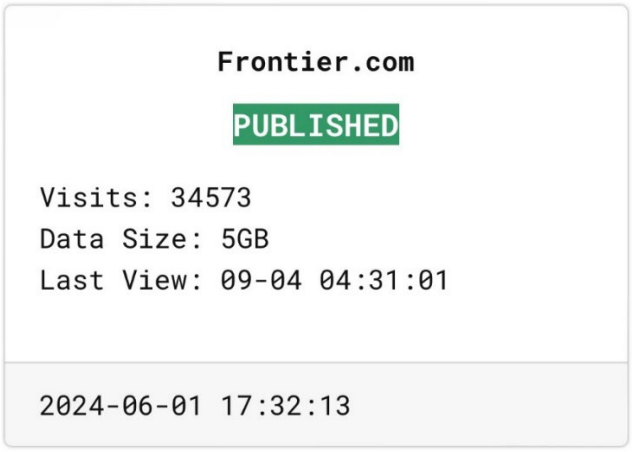
45. Frontier also failed to disclose in the Notice Letters that the notorious RansomHub hacker group had claimed responsibility for the Data Breach, or that RansomHub had published the trove of stolen Private Information on its dark web leak site for any number of unknown and nefarious actors to take and further misuse.

46. Thus, Frontier's purported disclosure amounts to no real disclosure at all, as it fails to inform Plaintiffs and Class Members of the Data Breach's critical facts with any degree of

specificity. Without these details, Plaintiffs' and Class Members' ability to mitigate the harms resulting from the Data Breach was and is severely diminished.

47. As shown by the (redacted) screenshot below, RansomHub published the Private Information stolen in the Data Breach, including Frontier's customers' full names, dates of birth, physical addresses, Social Security numbers, email addresses, subscription statuses, and service notes, on its dark web leak site:

48. As shown by the screenshot below, as of September 4, 2024, Plaintiffs' and Class Members' Private Information had already been viewed on RansomHub's dark web page over 34,000 times:



49. Upon information and belief, RansomHub first breached Frontier's network and exfiltrated Plaintiffs' and Class Members' Private Information stored in un-encrypted form therein, then encrypted Frontier systems once the Private Information was exfiltrated, dropping a ransom note during encryption.

50. Frontier could have prevented this Data Breach by properly securing and encrypting the files and file servers containing Plaintiffs' and Class Members' Private Information and training its employees on standard cybersecurity practices.

51. For example, if Frontier had implemented industry standard logging, monitoring, and alerting systems—basic technical safeguards that any PII-collecting company is expected to employ—then cybercriminals would not have been able to perpetrate prolonged malicious activity in Frontier's network systems without alarm bells going off, including the reconnaissance necessary to identify where Frontier stored PII, installation of malware or other methods of establishing persistence and creating a path to exfiltrate data, staging data in preparation for exfiltration, and then exfiltrating that data outside of Frontier's system without being caught.

52. Frontier would have recognized the malicious activities detailed in the preceding paragraph if it bothered to implement basic monitoring and detection systems, which then would have stopped the Data Breach or greatly reduced its impact.

53. Frontier did not use reasonable security procedures and practices appropriate to the sensitive and confidential nature of Plaintiffs' and Class Members' Private Information it collected and maintained, such as encrypting files containing Private Information or deleting Private Information from network systems when it is no longer needed, which caused that Private Information's unauthorized access and exfiltration in the Data Breach.

54. Additionally, according to the *#StopRansomware: RansomHub Ransomware* whitepaper published by CISA, RansomHub typically gains initial access to a targeted network through common techniques like phishing emails or exploiting known vulnerabilities in internet-facing systems.[8] Phishing is a tactic that uses social engineering to send emails containing malicious attachments to targeted organizations or individuals,[9] and relies on user execution (like opening an email or downloading an attachment) to gain access.[10]

55. CISA recommends rudimentary actions that businesses like Frontier should take immediately to mitigate cyber threats from RansomHub: (a) installing updates for operating systems, software, and firmware as soon as they are released; (b) requiring phishing-resistant multi-factor authentication ("MFA") (i.e., non-SMS text based) for as many services as possible; and (c) training users to recognize and report phishing attempts.[11]

56. Upon information and belief, Frontier failed to install updates for operating systems, software, and firmware as soon as they were released. Had Frontier installed such updates at its first opportunity as was standard and advised, the Data Breach would not have occurred, or would

---

[8] *Id*.

[9] *See* Phishing, MITRE ATT&CK (March 1, 2024), available at https://attack.mitre.org/versions/v15/techniques/T1566/ (last accessed July 9, 2024).

[10] *See* Phishing, MITRE ATT&CK (April 12, 2024), available at https://attack.mitre.org/versions/v15/techniques/T1204/ (last accessed July 9, 2024).

[11] #StopRansomware: RansomHub Ransomware, CISA (Aug. 29, 2024), available at https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-242a (last visited Sept. 4, 2024).

have at least been mitigated.

57. Further, upon information and belief, Frontier failed to require phishing-resistant MFA where possible or adequately train its employees to recognize and report phishing attempts. Had Frontier required phishing-resistant MFA, and/or trained its employees on reasonable and basic cybersecurity topics like common phishing techniques or indicators of a potentially malicious event, RansomHub would not have been able to carry out the Data Breach through phishing.

58. As a result of Frontier's failures, Plaintiffs' and Class Members' Private Information was stolen in the Data Breach when criminal RansomHub hackers accessed and acquired files in Frontier's computer systems storing that sensitive data in unencrypted form.

59. Frontier's tortious conduct and breach of contractual obligations, as detailed herein, are evidenced by its failure to recognize the Data Breach until cybercriminals had already accessed Plaintiffs' and Class Members' Private Information, meaning Frontier had no effective means in place to detect and prevent attempted cyberattacks.

C. Frontier Knew or Should Have Known of the Risk of a Cyber Attack Because Businesses in Possession of Private Information are Particularly Suspectable.

60. Frontier's negligence, including its gross negligence, in failing to safeguard Plaintiffs' and Class Members' Private Information is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

61. Private Information of the kind accessed in the Data Breach is of great value to cybercriminals as it can be used for a variety of unlawful and nefarious purposes, including ransomware, fraudulent misuse, and sale on the internet black market known as the dark web.

62. Private Information can also be used to distinguish, identify, or trace an individual's identity, such as his or her name, Social Security number, and financial records. This may be accomplished alone, or in combination with other personal or identifying information connected

or linked to an individual such as his or her birthdate, birthplace, and mother's maiden name.

63. Data thieves regularly target entities that store PII like Frontier due to the highly sensitive information they maintain. Frontier knew and understood that Plaintiffs' and Class Members' Private Information is valuable and highly sought after by criminal parties who seek to illegally monetize it through unauthorized access.

64. Cyberattacks against institutions such as Frontier are targeted and frequent. According to Contrast Security's 2023 report, "Cyber Bank Heists: Threats to the financial sector," "[o]ver the past year, attacks have included banking trojans, ransomware, account takeover, theft of client data and cybercrime cartels deploying 'trojanized' finance apps to deliver malware in spear-phishing campaigns."[12]

65. Cyberattacks by the RansomHub group in particular, as in this Data Breach, have been particularly prevalent in recent months. According to CISA, since February 2024 "RansomHub has encrypted and exfiltrated data from at least 210 victims representing the water and wastewater, information technology, government services and facilities, healthcare and public health, emergency services, food and agriculture, financial services, commercial facilities, critical manufacturing, transportation, and communications critical infrastructure sectors."[13]

66. According to the Identity Theft Resource Center's report covering the year 2021, "the overall number of data compromises (1,862) is up more than 68 percent compared to 2020. The new record number of data compromises is 23 percent over the previous all-time high (1,506) set in 2017. The number of data events that involved sensitive information (Ex: Social Security

[12] Tom Kellermann, *Cyber Bank Heists: Threats to the financial sector*, at 5, CONTRAST SECURITY https://www.contrastsecurity.com/hubfs/Cyber%20Bank%20Heists%20Report%2020 23.pdf (last accessed July 8, 2024).

[13] *See #StopRansomware: RansomHub Ransomware* FED. BUREAU INVESTIGATION, ET AL. (Aug. 29, 2024), available at https://www.cisa.gov/sites/default/files/2024-08/aa24-242a-stopransomware-ransomhub-ransomware_0.pdf (last accessed Sept. 4, 2024).

numbers) increased slightly compared to 2020 (83 percent vs. 80 percent)."[14]

67. The increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Frontier's industry, including Frontier itself. According to IBM's 2022 report, "[f]or 83% of companies, it's not if a data breach will happen, but when."[15]

68. Despite the prevalence of public announcements of data breach and data security compromises, Frontier failed to take appropriate steps to protect Plaintiffs' and Class Members' Private Information from being compromised in this Data Breach.

69. As a national service provider in possession of millions of customers' Private Information, Frontier knew, or should have known, the importance of safeguarding the Private Information entrusted to it by Plaintiffs and Class Members and of the foreseeable consequences they would suffer if Frontier's data security systems were breached. Such consequences include the significant costs imposed on Plaintiffs and Class Members due to the unauthorized exposure of their Private Information to criminal actors. Nevertheless, Frontier failed to take adequate cybersecurity measures to prevent the Data Breach or the foreseeable injuries it caused.

70. Given the nature of the Data Breach, it was foreseeable that Plaintiffs' and Class Members' Private Information compromised therein would be targeted by hackers and cybercriminals, including RansomHub specifically, for use in variety of different injurious ways. Indeed, the cybercriminals who possess Plaintiffs' and Class Members' Private Information can easily obtain their tax returns or open fraudulent credit card accounts in Plaintiffs' and Class Members' names.

---

[14] *See* Identity Theft Resource Center, *2021 Annual Data Breach Report Sets New Record for Number of Compromises*, ITRC (Jan. 24, 2022), https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises.

[15] IBM, *Cost of a data breach 2022: A million-dollar race to detect and respond*, https://www.ibm.com/reports/data-breach (last accessed July 8, 2024).

71. Frontier was, or should have been, fully aware of the unique type and the significant volume of data on Frontier's network server(s) and systems, amounting to millions of individuals' detailed Private Information, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

72. Plaintiffs and Class Members were the foreseeable and probable victims of Frontier's inadequate security practices and procedures. Frontier knew or should have known of the inherent risks in collecting and storing Private Information and the critical importance of providing adequate security for that data.

73. The breadth of data compromised in the Data Breach makes the information particularly valuable to criminals and leaves Plaintiffs and Class Members especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and more.

D. Frontier is Required, But Failed, to Comply with FTC Rules and Guidance.

74. The FTC has promulgated numerous guides that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

75. In 2016 the FTC updated its publication, *Protecting Personal Information: A Guide for Business*,[16] which established cyber-security guidelines for businesses like Frontier. These guidelines note that businesses should protect the Private Information that they keep; properly dispose of Private Information that is no longer needed; encrypt Private Information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

[16] *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (2016),https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed May 8, 2024).

76. The FTC's guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[17]

77. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

78. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect third parties' confidential data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45 *et seq*. Orders resulting from these actions further clarify the measures business like Frontier must undertake to meet their data security obligations.

79. Such FTC enforcement actions include those against businesses that fail to adequately protect customer data, like Frontier here. *See, e.g.*, *In the Matter of LabMD, Inc*., 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

80. 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

[17] *Id.*

by businesses like Frontier of failing to use reasonable measures to protect Private Information they collect and maintain from consumers. The FTC publications and orders described above also form part of the basis of Frontier's duty in this regard.

81. The FTC has also recognized that personal data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis and profit."[18]

82. Frontier failed to properly implement basic data security practices, in violation of its duties under the FTC Act.

83. Frontier's failure to comply with industry standards or employ reasonable and appropriate measures to protect against unauthorized access to and disclosure of Plaintiffs' and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

E. Frontier Failed to Comply with Industry Standards.

84. A number of published industry and national best practices are widely used as a go-to resource when developing an institution's cybersecurity standards.

85. The Center for Internet Security's (CIS) Critical Security Controls (CSC) recommends certain best practices to adequately secure data and prevent cybersecurity attacks, including Critical Security Controls of Inventory and Control of Enterprise Assets, Inventory and Control of Software Assets, Data Protection, Secure Configuration of Enterprise Assets and Software, Account Management, Access Control Management, Continuous Vulnerability

[18] Statement of FTC Commissioner Pamela Jones Harbour (Remarks Before FTC Exploring Privacy Roundtable), http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf.

Management, Audit Log Management, Email and Web Browser Protections, Malware Defenses, Data Recovery, Network Infrastructure Management, Network Monitoring and Defense, Security Awareness and Skills Training, Service Provider Management, Application Software Security, Incident Response Management, and Penetration Testing.[19]

86. The National Institute of Standards and Technology ("NIST") also recommends certain practices to safeguard systems, such as the following:

a. Control who logs on to your network and uses your computers and other devices.

b. Use security software to protect data.

c. Encrypt sensitive data, at rest and in transit.

d. Conduct regular backups of data.

e. Update security software regularly, automating those updates if possible.

f. Have formal policies for safely disposing of electronic files and old devices.

g. Train everyone who uses your computers, devices, and network about cybersecurity. You can help employees understand their personal risk in addition to their crucial role in the workplace.

87. Further still, CISA makes specific recommendations to organizations to guard against cybersecurity attacks, including (a) reducing the likelihood of a damaging cyber intrusion by validating that "remote access to the organization's network and privileged or administrative access requires multi-factor authentication, [e]nsur[ing] that software is up to date, prioritizing updates that address known exploited vulnerabilities identified by CISA[,] [c]onfirm[ing] that the organization's IT personnel have disabled all ports and protocols that are not essential for business

[19] *See* Rapid7, "CIS Top 18 Critical Security Controls Solutions," available at https://www.rapid7.com/solutions/compliance/critical-controls/ (last acc. Feb. 9, 2024).

purposes," and other steps; (b) taking steps to quickly detect a potential intrusion, including "[e]nsur[ing] that cybersecurity/IT personnel are focused on identifying and quickly assessing any unexpected or unusual network behavior [and] [e]nabl[ing] logging in order to better investigate issues or events[;] [c]onfirm[ing] that the organization's entire network is protected by antivirus/antimalware software and that signatures in these tools are updated," and (c) "[e]nsur[ing] that the organization is prepared to respond if an intrusion occurs," and other steps.[20]

88. Upon information and belief, Frontier failed to implement industry-standard cybersecurity measures, including by failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 2.0 (including PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04) and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established frameworks for reasonable cybersecurity readiness, and by failing to comply with other industry standards for protecting Plaintiffs' and Class Members' Private Information, resulting in the Data Breach.

F. Frontier Owed Plaintiffs and Class Members a Common Law Duty to Safeguard their Private Information.

89. In addition to its obligations under federal and state laws, Frontier owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Frontier's duty owed to Plaintiffs and Class Members obligated it to provide reasonable data security, including consistency with industry standards and requirements, and to ensure that its computer systems,

[20] CISA, *Shields Up: Guidance for Organizations*, https://www.cisa.gov/shields-guidance-organizations (last accessed July 8, 2024).

networks, and protocols adequately protected Plaintiffs' and Class Members' Private Information.

90. Frontier owed a duty to Plaintiffs and Class Members to create and implement reasonable data security practices and procedures to protect the Private Information in its possession, including adequately training its employees and others who accessed Private Information within its computer systems on how to adequately protect Private Information.

91. Frontier owed a duty to Plaintiffs and Class Members to implement processes that would detect a compromise of Private Information in a timely manner.

92. Frontier owed a duty to Plaintiffs and Class Members to act upon data security warnings and alerts in a timely fashion.

93. Frontier owed a duty to Plaintiffs and Class Members to disclose in a timely and accurate manner when and how the Data Breach occurred.

94. Frontier owed these duties of care to Plaintiffs and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

95. Frontier tortiously failed to take the precautions required to safeguard and protect Plaintiffs' and Class Members' Private Information from unauthorized disclosure. Frontier's actions and omissions represent a flagrant disregard of Plaintiffs' and Class Members' rights.

G. Plaintiffs and Class Members Suffered Common Injuries and Damages due to Frontier's Deficient Data Security and the Resulting Data Breach.

96. Frontier's failure to implement or maintain adequate data security measures for Plaintiffs' and Class Members' Private Information directly and proximately caused injuries to Plaintiffs and Class Members by the resulting disclosure of their Private Information to a criminal ransomware group in the Data Breach.

97. Frontier's conduct, which allowed the Data Breach to occur, caused Plaintiffs and Class Members significant injuries and harm in several ways. Plaintiffs and Class Members must

immediately devote time, energy, and money to (a) closely monitor their medical statements, bills, records, and credit and financial accounts; (b) change login and password information on any sensitive account even more frequently than they already do; (c) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and (d) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

98. The unencrypted Private Information of Plaintiffs and Class Members compromised in the Data Breach has ***already*** been published and disseminated on the dark web by RansomHub, where as of September 3, 2024, it had been viewed over 34,000 times. Unauthorized actors with bad intentions can now easily access Plaintiffs' and Class Members' Private Information—and thousands have already done so.

99. The ramifications of Frontier's failure to keep the Private Information of Plaintiffs and Class Members secure are long lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years.

100. Plaintiffs and Class Members are also at a continued risk because their Private Information remains in Frontier's systems, which have already been shown to be susceptible to compromise and are subject to further attack so long as Frontier fails to undertake the necessary and appropriate security and training measures to protect its customers' Private Information.

101. As a result of Frontier's ineffective and inadequate data security practices, the consequential Data Breach, and the foreseeable outcome of Plaintiffs' and Class Members' Private Information ending up in criminals' possession, Plaintiffs and Class Members have suffered and will continue to suffer the following injuries and damages, without limitation: (a) invasion of privacy; (b) financial costs incurred mitigating the materialized risk and imminent threat of identity

theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (d) financial costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) deprivation of value of their Private Information; (g) loss of the benefit of their bargain with Frontiers; (h) emotional distress including anxiety and stress in dealing with the Data Breach's aftermath; (i) an increase in spam and scam robocalls, emails, and texts; and (j) the continued risk to their sensitive Private Information, which remains in Frontier's possession and subject to further unauthorized disclosures so long as Frontier fails to undertake appropriate and adequate measures to protect it.

Present and Ongoing Risk of Identity Theft

102. Given the publication of their Private Information on the dark web and the fraudulent misuse of such Private Information that has already taken place, as set forth in greater detail below, Plaintiffs and Class Members are at a heightened risk of identity theft for years to come because of the Data Breach.

103. 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.

104. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the data by selling it on the internet black market to other criminals, who then utilize it to commit a variety of identity theft related crimes discussed below. Thus, unauthorized actors can, and will, now easily access and misuse Plaintiffs' and Class Members' Private Information due to the Data Breach.

105. The dark web is an unindexed layer of the internet that requires special software or authentication to access. Criminals in particular favor the dark web as it offers a degree of anonymity to visitors and website publishers. Unlike the traditional or "surface" web, dark web

users need to know the web address of the website they wish to visit in advance. For example, on the surface web, the CIA's web address is cia.gov, but on the dark web the CIA's web address is ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion. This prevents dark web marketplaces from being easily monitored by authorities or accessed by those not in the know.

106. A sophisticated black market exists on the dark web where criminals can buy or sell malware, firearms, drugs, and frequently, PII like the Private Information at issue here. The digital character of information stolen in data breaches lends itself to dark web transactions because it is immediately transmissible over the internet and the buyer and seller can retain their anonymity. The sale of a firearm or drugs on the other hand requires a physical delivery address. Nefarious actors can readily purchase usernames and passwords for online streaming services, stolen financial information and account login credentials, and Social Security numbers, dates of birth, and medical information.

107. In addition, unencrypted and detailed Private Information may fall into the hands of companies that will use it for targeted marketing without the approval of Plaintiffs and Class Members.

108. Social Security numbers in particular are among the worst kinds of personal information to have stolen because they may be put to numerous serious fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to

> get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[21]

109. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

110. Even then, new Social Security number may not be effective, as "[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."[22]

111. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant issued in the victim's name. And the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for credit lines.[23]

112. Further, because a person's identity is akin to a puzzle with multiple data points,

---

[21] Social Security Administration, *Identity Theft and Your Social Security Number*, available at: https://www.ssa.gov/pubs/EN-05-10064.pdf.

[22] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited Aug. 23, 2024).

[23] *Identity Theft and Your Social Security Number*, Social Security Administration, 1 (2018), available at https://www.ssa.gov/pubs/EN-05-10064.pdf.

the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or to track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

113. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data breaches are often the starting point for these additional targeted attacks on the victims.

114. One such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of "Fullz" packages.[24]

115. With "Fullz" packages, cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy to assemble complete dossiers on individuals.

116. The development of "Fullz" packages means here that the stolen Private

[24] 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 those credentials. Fullz are usually pricier than standard credit card credentials, 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.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm (last visited Feb. 26, 2024).

Information from the Data Breach can easily be used to link and identify it to Plaintiffs' and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information that was exfiltrated in the Data Breach, criminals can still easily create a Fullz package and sell it at a higher price to unscrupulous operators (such as illegal and scam telemarketers) and other nefarious actors over and over. That is exactly what is happening to Plaintiffs and Class Members, and it is reasonable for any trier of fact, including this Court or a jury, to find that their stolen Private Information is being misused, and that such misuse is traceable to the Data Breach.

117. Bad actors can also use the Private Information stolen in this Data Breach to access a victim's financial accounts. Identity thieves can impersonate victims by using call spoofing services to falsify information transmitted to a call recipient's caller ID, disguising the identity thief's phone number as the victim's. If the bad actor knows what bank or credit card company the victim uses, it can use spoofing to call the victim's financial institution while masquerading as the victim's phone number to the financial institution's caller ID, using other Private Information about the victim (like the victim's Social Security number) to falsely verify the victim's identity if prompted. Posing as the victim during such calls, identity thieves can obtain information like the victim's account number from the financial institution, or change the victim's online banking or credit card account login information.

118. Even if an identity thief does not know what bank or credit card company the victim uses, the Private Information stolen in the Data Breach can be used to obtain that information. For example, with the Private Information taken in this Data Breach—name, date of birth, address, contact information, and Social Security number—a fraudster can obtain the victim's free

consumer disclosure report from a credit reporting agency. These consumer disclosure reports list information about the consumer's financial accounts, including bank addresses, routing numbers, and partial bank account numbers.

119. Similarly, identity thieves can use a victim's name, date of birth, address, contact information, and Social Security number—all Private Information stolen in this Data Breach—to obtain a free copy of the victim's credit report, which contains information like the victim's credit card accounts (with partial card numbers) and banking institutions, as well as additional information about the victim like account balances and previous addresses.

120. Thus, even if a victim's bank account or credit card information was not compromised in this Data Breach, it is entirely possible for bad actors to use the Private Information obtained about Plaintiffs and Class Members to perpetrate bank or credit card fraud against them.

121. Victims of identity theft can suffer from both direct and indirect financial losses. According to a research study published by the Department of Justice,

> A direct financial loss is the monetary amount the offender obtained from misusing the victim's account or personal information, including the estimated value of goods, services, or cash obtained. It includes both out-of-pocket loss and any losses that were reimbursed to the victim. An indirect loss includes any other monetary cost caused by the identity theft, such as legal fees, bounced checks, and other miscellaneous expenses that are not reimbursed (e.g., postage, phone calls, or notary fees). All indirect losses are included in the calculation of out-of-pocket loss.[25]

122. 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 that

[25] Erika Harrell, *Bureau of Just. Stat.*, U.S. DEP'T OF JUST., NCJ 256085, *Victims of Identity Theft*, 2018 I (2020) https://bjs.ojp.gov/content/pub/pdf/vit18.pdf (last accessed Jan. 23, 2024).

year, resulting in more than $3.5 billion in losses to individuals and business victims.[26]

123. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

124. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims must spend a considerable time repairing the damage caused by the theft of their Private Information. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

125. Further complicating the issues faced by victims of identity theft, data thieves may wait years before using stolen Private Information. To protect themselves, Plaintiffs and Class Members will need to remain vigilant for years or even decades to come.

Loss of Time to Mitigate the Risk of Identify Theft and Fraud

126. As a result of the recognized risk of identity theft, when a data breach occurs, and an individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm—yet the asset of time has been lost.

127. In the likely event that Plaintiffs and Class Members experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding

[26] *See* https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120.

data breaches in which it noted that victims of identity theft will face substantial costs and time to repair the damage to their good name and credit record.

128. Thus, due to the actual and imminent risk of identity theft, Plaintiffs and Class Members must monitor their financial accounts for many years to mitigate that harm.

129. Plaintiffs and Class Members have spent time, and will spend additional time in the future, on a variety of prudent actions, such as placing "freezes" and "alerts" with credit reporting agencies, contacting financial institutions, closing or modifying financial accounts, changing passwords, reviewing and monitoring credit reports and accounts for unauthorized activity, and filing police reports, which may take years to discover.

130. These efforts are consistent with the steps that FTC recommends that data breach victims take several steps 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.[27]

131. Once Private Information is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiffs and Class Members will need to maintain these heightened measures for years, and possibly their entire lives, due to Frontier's conduct and the resulting Data Breach.

Diminished Value of Private Information

132. Private Information is a valuable property right. Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy

[27] *See* FTC, *Identity Theft.gov*, https://www.identitytheft.gov/Steps (last visited Feb. 26, 2024).

prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

133. For example, drug and medical device manufacturers, pharmacies, hospitals, and other healthcare service providers often purchase Private Information on the black market for the purpose of target-marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

134. Private Information can sell for hundreds of dollars per record on the dark web.[28]

135. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion. In fact, consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50 a year.[29]

136. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished in its value by its unauthorized and likely release onto the dark web, where holds significant value for threat actors. Thus, Plaintiffs and Class Members have been deprived of the opportunity to use or profit from their own Private Information as they choose.

137. However, this transfer of value occurred without any consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the Private

[28] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/.
[29] Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html.

Information is now readily available, and the rarity of the data has been lost, thereby causing additional diminution of value.

Reasonable and Necessary Future Costs of Credit and Identify Theft Monitoring

138. To date, Frontier has done little to provide Plaintiffs and Class Members with relief for the damages they have suffered and will continue to suffer for years due to the Data Breach.

139. RansomHub has already published the Private Information exfiltrated in the Data Breach to its dark web leak site. Given the type of Private Information involved in this Data Breach, and the *modus operandi* of cybercriminals, there is a strong probability that entire batches of stolen Private Information have been or will be further disseminated on the black market/dark web for sale and purchase by bad actors intending to utilize it for identity theft crimes—*e.g.*, opening bank and other accounts in the victims' names to make purchases or to launder money, filing false tax returns, taking out loans or lines of credit, or filing false unemployment claims.

140. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

141. The Private Information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer breach, where victims can easily cancel or close accounts. The Private Information disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

142. Consequently, Plaintiffs and Class Members are at a present and ongoing risk of fraud and identity theft for many years into the future, if not forever.

143. The retail cost of credit monitoring and identity theft monitoring can cost $200 or more a year per Class Member. This is a reasonable and necessary cost to protect Class Members from the risk of identity theft that arose from Frontier's Data Breach. This is a future cost for a minimum of five years that Plaintiffs and Class Members would not need to bear but for Frontier's failure to safeguard their Private Information.

Lost Benefit of the Bargain

144. Furthermore, Frontier's poor data security deprived Plaintiffs and Class Members of the benefit of their bargain.

145. When agreeing to provide their Private Information (which was a condition precedent to obtain internet products and services from Frontier), and pay Frontier, Plaintiffs and Class Members as consumers understood and expected that they were, in part, paying a premium for services and data security to protect the Private Information they were required to provide.

146. In fact, Frontier did not provide the expected and bargained-for data security. Accordingly, Plaintiffs and Class Members received products and services that were of a lesser value than what they reasonably expected to receive under the bargains struck with Frontier.

V. PLAINTIFFS' EXPERIENCES AND INJURIES

Plaintiff Brian Carolus

147. Plaintiff Brian Carolus is a current customer of Frontier. As a condition of receiving internet products and services from Frontier, Plaintiff Carolus was required to supply Frontier with his Private Information, including his name, contact information, Social Security number, usage information, and other sensitive information.

148. Plaintiff Carolus greatly values his privacy and is very careful about sharing his sensitive Private Information. Plaintiff Carolus diligently protects his Private Information and stores any documents containing Private Information in a safe and secure location. He has never

knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

149. Plaintiff Carolus would not have provided his Private Information to Frontier had he known it would be kept using inadequate data security and vulnerable to a cyberattack.

150. At the time of the Data Breach—in or around April 2024—Frontier retained Plaintiff Carolus's Private Information in its network systems with inadequate data security, causing Plaintiff Carolus's Private Information to be accessed and exfiltrated by RansomHub in the Data Breach.

151. On or about June 6, 2024, Plaintiff Carolus received Frontier's Notice Letter informing that his Private Information was accessed and exposed to unauthorized hackers in the Data Breach. According to the Notice Letter, hackers acquired files containing Plaintiff Carolus's sensitive Private Information, including his name, date of birth, and Social Security number.

152. Plaintiff Carolus has made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff Carolus now monitors his financial and credit statements multiple times a week and has spent hours dealing with the Data Breach, valuable time he otherwise would have spent on other activities.

153. Plaintiff Carolus's Private Information compromised in the Data Breach has already been misused to commit identity theft and fraud. Specifically, in May 2024, Plaintiff Carolus received a letter from the IRS advising him that an unknown actor had used his Social Security number to fraudulently apply for employment, without Plaintiff Carolus's knowledge or authorization. Prior to this incident, Plaintiff Carolus to his knowledge had never been the victim

of identity theft or fraud.

154. Plaintiff Carolus further anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Due to the Data Breach, Plaintiff Carolus is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

155. The risk of identity theft is impending and has materialized, as Plaintiff Carolus's and Class Members' Private Information was targeted, accessed, misused, and disseminated on the dark web by RansomHub, a notorious criminal organization.

156. The Data Breach has caused Plaintiff Carolus to suffer fear, anxiety, and stress about his Private Information now being in the hands of cybercriminals, which has been compounded by the fact that Frontier still has not fully informed him of key details about the Data Breach's occurrence or the information stolen.

157. Moreover, since the Data Breach Plaintiff Carolus has experienced suspicious spam calls and texts using his compromised Private Information, and believes this to be an attempt to secure additional information from or about him.

Plaintiff Adrian Graham

158. Plaintiff Adrian Graham is a current customer of Frontier. As a condition of receiving internet products and services from Frontier, Plaintiff Graham was required to supply Frontier with his Private Information, including his name, contact information, Social Security number, usage information, and other sensitive information.

159. Plaintiff Graham greatly values his privacy and is very careful about sharing his sensitive Private Information. Plaintiff Graham diligently protects his Private Information and stores any documents containing Private Information in a safe and secure location. He has never

knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

160. Plaintiff Graham would not have provided his Private Information to Frontier had he known it would be kept using inadequate data security and vulnerable to a cyberattack.

161. At the time of the Data Breach—in or around April 2024—Frontier retained Plaintiff Graham's Private Information in its network systems with inadequate data security, causing Plaintiff Graham's Private Information to be accessed and exfiltrated by RansomHub in the Data Breach.

162. On or about June 6, 2024, Plaintiff Graham received Frontier's Notice Letter informing that his Private Information was accessed and exposed to unauthorized hackers in the Data Breach. According to the Notice Letter, hackers acquired files containing Plaintiff Graham's sensitive Private Information, including his name, date of birth, and Social Security number.

163. Plaintiff Graham has made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff Graham now monitors his financial and credit statements multiple times a week and has spent hours dealing with the Data Breach, valuable time he otherwise would have spent on other activities.

164. Plaintiff Graham's Private Information compromised in the Data Breach has already been misused to commit identity theft and fraud. Specifically, since the Data Breach Plaintiff Graham experienced identity theft in the form of an unauthorized charge to his debit card made by an unknown actor. Due to the fraudulent charge, Plaintiff Graham was forced to cancel his debit card, costing him further time and inconvenience.

165. Plaintiff Graham further anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Due to the Data Breach, Plaintiff Graham is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

166. The risk of identity theft is impending and has materialized, as Plaintiff Graham's and Class Members' Private Information was targeted, accessed, misused, and disseminated on the dark web by RansomHub, a notorious criminal organization.

167. The Data Breach has caused Plaintiff Graham to suffer fear, anxiety, and stress, particularly that his Private Information is now in the hands of cybercriminals and that his identity will continue to be stolen, which has been compounded by the fact that Frontier still has not fully informed him of key details about the Data Breach's occurrence or the information stolen.

168. Moreover, since the Data Breach Plaintiff Graham has experienced suspicious spam calls and texts using his compromised Private Information, and believes this to be an attempt to secure additional information from or about him.

Plaintiff Christopher Miller

169. Plaintiff Christopher Miller is a former customer of Frontier. As a condition of receiving internet products and services from Frontier, Plaintiff Miller was required to supply Frontier with his Private Information, including his name, contact information, Social Security number, usage information, and other sensitive information.

170. Plaintiff Miller greatly values his privacy and is very careful about sharing his sensitive Private Information. Plaintiff Miller diligently protects his Private Information and stores any documents containing Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other

unsecured source.

171. Plaintiff Miller would not have provided his Private Information to Frontier had he known it would be kept using inadequate data security and vulnerable to a cyberattack.

172. At the time of the Data Breach—in or around April 2024—Frontier retained Plaintiff Miller's Private Information in its network systems with inadequate data security, causing Plaintiff Miller's Private Information to be accessed and exfiltrated by RansomHub in the Data Breach.

173. On or about June 6, 2024, Plaintiff Miller received Frontier's Notice Letter informing that his Private Information was accessed and exposed to unauthorized hackers in the Data Breach. According to the Notice Letter, hackers acquired files containing Plaintiff Miller's sensitive Private Information, including his name, date of birth, and Social Security number.

174. Plaintiff Miller has made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff Miller now monitors his financial and credit statements multiple times a week and has spent hours dealing with the Data Breach, valuable time he otherwise would have spent on other activities.

175. Plaintiff Miller's Private Information compromised in the Data Breach has already been misused to commit identity theft and fraud. Specifically, following the Data Breach Plaintiff Miller experienced identity theft in the form of several pay day loans taken out in his name, which he did not recognize or authorize. Prior to this incident, Plaintiff Miller to his knowledge had never been the victim of identity theft or fraud.

176. Plaintiff Miller further anticipates spending considerable time and money on an

ongoing basis to try to mitigate and address harms caused by the Data Breach. Due to the Data Breach, Plaintiff Miller is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

177. The risk of identity theft is impending and has materialized, as Plaintiff Miller's and Class Members' Private Information was targeted, accessed, misused, and disseminated on the dark web by RansomHub, a notorious criminal organization.

178. The Data Breach has caused Plaintiff Miller to suffer fear, anxiety, and stress, particularly that Private Information is now in criminals' possession, which has been compounded by the fact that Frontier still has not fully informed him of key details about the Data Breach's occurrence or the information stolen.

179. Moreover, since the Data Breach Plaintiff Miller has experienced suspicious spam calls and texts using his compromised Private Information, and believes this be an attempt to secure additional information from or about him.

Plaintiff Lauren Morgan

180. Plaintiff Lauren Morgan is a current customer of Frontier. As a condition of receiving internet products and services from Frontier, Plaintiff Lauren Morgan was required to supply Frontier with her Private Information, including her name, contact information, Social Security number, usage information, and other sensitive information.

181. Plaintiff Lauren Morgan greatly values her privacy and is very careful about sharing her sensitive Private Information. Plaintiff Lauren Morgan diligently protects her Private Information and stores any documents containing Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

182. Plaintiff Lauren Morgan would not have provided her Private Information to Frontier had she known it would be kept using inadequate data security and vulnerable to a cyberattack.

183. At the time of the Data Breach—in or around April 2024—Frontier retained Plaintiff Lauren Morgan's Private Information in its network systems with inadequate data security, causing Plaintiff Lauren Morgan's Private Information to be accessed and exfiltrated by RansomHub in the Data Breach.

184. On or about June 6, 2024, Plaintiff Lauren Morgan received Frontier's Notice Letter informing that her Private Information was accessed and exposed to unauthorized hackers in the Data Breach. According to the Notice Letter, hackers acquired files containing Plaintiff Morgan's sensitive Private Information, including her name, date of birth, and Social Security number.

185. Plaintiff Lauren Morgan has made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff Lauren Morgan now monitors her financial and credit statements multiple times a week and has spent hours dealing with the Data Breach, valuable time she otherwise would have spent on other activities.

186. Plaintiff Lauren Morgan further anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Due to the Data Breach, Plaintiff Lauren Morgan is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

187. The risk of identity theft is impending and has materialized, as Plaintiff Morgan's and Class Members' Private Information was targeted, accessed, misused, and disseminated on the

dark web by RansomHub, a notorious criminal organization.

188. The Data Breach has caused Plaintiff Lauren Morgan to suffer fear, anxiety, and stress, particularly that criminals will misuse her Private Information to commit identity theft and fraud, which has been compounded by the fact that Frontier still has not fully informed her of key details about the Data Breach's occurrence or the information stolen.

189. Moreover, since the Data Breach Plaintiff Lauren Morgan has experienced suspicious spam calls and solicitations using her compromised Private Information, and believes this to be an attempt to secure additional information from or about her.

Plaintiff Marcelo Muto

190. Plaintiff Marcelo Muto is a former customer of Frontier. As a condition of receiving internet and/or cable products and services from Frontier, Plaintiff Muto was required to supply Frontier with his Private Information, including his name, contact information, Social Security number, usage information, and other sensitive information.

191. Plaintiff Muto greatly values his privacy and is very careful about sharing his sensitive Private Information. Plaintiff Muto diligently protects his Private Information and stores any documents containing Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

192. Plaintiff Muto would not have provided his Private Information to Frontier had he known it would be kept using inadequate data security and vulnerable to a cyberattack.

193. At the time of the Data Breach—in or around April 2024—Frontier retained Plaintiff Muto's Private Information in its network systems with inadequate data security, causing

Plaintiff Muto's Private Information to be accessed and exfiltrated by RansomHub in the Data Breach.

194. On or about June 6, 2024, Plaintiff Muto received Frontier's Notice Letter informing that his Private Information was accessed and exposed to unauthorized hackers in the Data Breach. According to the Notice Letter, hackers acquired files containing Plaintiff Muto's sensitive Private Information, including his name, date of birth, and Social Security number.

195. Plaintiff Muto has made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff Muto now monitors his financial and credit statements multiple times a week and has spent hours dealing with the Data Breach, valuable time he otherwise would have spent on other activities.

196. Plaintiff Muto's Private Information compromised in the Data Breach has already been misused to commit identity theft and fraud. Specifically, since the Data Breach Plaintiff Muto has experienced identity theft in the form of several unauthorized charges on his debit card. Due to the fraudulent charges, Plaintiff Muto was forced to close his debit card, costing him additional time and inconvenience.

197. Plaintiff Muto further anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Due to the Data Breach, Plaintiff Muto is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

198. The risk of identity theft is impending and has materialized, as Plaintiff Muto's and Class Members' Private Information was targeted, accessed, misused, and disseminated on the

dark web by RansomHub, a notorious criminal organization.

199. The Data Breach has caused Plaintiff Muto to suffer fear, anxiety, and stress, particularly due to the invasion of his privacy and his concern about the lasting effects of cybercriminals accessing his sensitive data, which has been compounded by the fact that Frontier still has not fully informed him of key details about the Data Breach's occurrence or the information stolen.

200. Moreover, since the Data Breach Plaintiff Muto has experienced suspicious spam calls and texts using his compromised Private Information, and believes this to be an attempt to secure additional information from or about him.

Plaintiff Ian Terrell

201. Plaintiff Ian Terrell is a current customer of Frontier. As a condition of receiving internet products and services from Frontier, Plaintiff Terrell was required to supply Frontier with his Private Information, including his name, contact information, Social Security number, usage information, and other sensitive information.

202. Plaintiff Terrell greatly values his privacy and is very careful about sharing his sensitive Private Information. Plaintiff Terrell diligently protects his Private Information and stores any documents containing Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

203. Plaintiff Terrell would not have provided his Private Information to Frontier had he known it would be kept using inadequate data security and vulnerable to a cyberattack.

204. At the time of the Data Breach—in or around April 2024—Frontier retained Plaintiff Terrell's Private Information in its network systems with inadequate data security, causing

Plaintiff Terrell's Private Information to be accessed and exfiltrated by RansomHub in the Data Breach.

205. On or about June 6, 2024, Plaintiff Terrell received Frontier's Notice Letter informing that his Private Information was accessed and exposed to unauthorized hackers in the Data Breach. According to the Notice Letter, hackers acquired files containing Plaintiff Terrell's sensitive Private Information, including his name, date of birth, and Social Security number.

206. Plaintiff Terrell has made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Among other things, Plaintiff Terrell has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing financial account statements and credit card statements, corresponding with his bank to dispute fraudulent transactions, and taking other protective and ameliorative steps in response to the Data Breach. Plaintiff Terrell now monitors his financial and credit statements multiple times a week and has spent hours dealing with the Data Breach, valuable time he otherwise would have spent on other activities.

207. Plaintiff Terrell's Private Information compromised in the Data Breach has already been misused to commit identity theft and fraud. Specifically, since the Data Breach Plaintiff Terrell has experienced identity theft in the form of fraudulent and unauthorized charges made on his debit card in May 2024.

208. Plaintiff Terrell further anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Due to the Data

Breach, Plaintiff Terrell is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

209. The risk of identity theft is impending and has materialized, as Plaintiff Terrell's and Class Members' Private Information was targeted, accessed, misused, and disseminated on the dark web by RansomHub, a notorious criminal organization.

210. The Data Breach has caused Plaintiff Terrell to suffer fear, anxiety, and stress, particularly due to the invasion of his privacy and his concern about damage to his credit and the identity theft he has already been experienced, which has been compounded by the fact that Frontier still has not fully informed him of key details about the Data Breach's occurrence or the information stolen.

211. Moreover, since the Data Breach Plaintiff Terrell has experienced suspicious spam calls and texts using his compromised Private Information, and believes this to be an attempt to secure additional information from or about him.

Plaintiff Richard Retter

212. Plaintiff Richard Retter is a former customer of Frontier. As a condition of receiving internet products and services from Frontier, Plaintiff Retter was required to supply Frontier with his Private Information, including his name, contact information, Social Security number, usage information, and other sensitive information.

213. Plaintiff Retter greatly values his privacy and is very careful about sharing his sensitive Private Information. Plaintiff Retter diligently protects his Private Information and stores any documents containing Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

214. Plaintiff Retter would not have provided his Private Information to Frontier had he known it would be kept using inadequate data security and vulnerable to a cyberattack.

215. At the time of the Data Breach—in or around April 2024—Frontier retained Plaintiff Retter's Private Information in its network systems with inadequate data security, causing Plaintiff Retter's Private Information to be accessed and exfiltrated by RansomHub in the Data Breach.

216. On or about June 6, 2024, Plaintiff Retter received Frontier's Notice Letter informing that his Private Information was accessed and exposed to unauthorized hackers in the Data Breach. According to the Notice Letter, hackers acquired files containing Plaintiff Retter's sensitive Private Information, including his name, date of birth, and Social Security number.

217. Plaintiff Retter has made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Among other things, Plaintiff Retter has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing financial account statements and credit card statements, and taking other protective and ameliorative steps. Plaintiff Retter now monitors his financial and credit statements multiple times a week and has spent hours dealing with the Data Breach, valuable time he otherwise would have spent on other activities.

218. Plaintiff Retter's Private Information compromised in the Data Breach has already been misused, as evidenced by notifications Plaintiff Retter received since the Data Breach alerting that his Social Security number had been found on the dark web.

219. Plaintiff Retter further anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Due to the Data Breach, Plaintiff Retter is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

220. The risk of identity theft is impending and has materialized, as Plaintiff Retter's and Class Members' Private Information was targeted, accessed, misused, and disseminated on the dark web by RansomHub, a notorious criminal organization.

221. The Data Breach has caused Plaintiff Retter to suffer fear, anxiety, and stress, particularly due to the invasion of his privacy and his Private Information's publication on the dark web, which has been compounded by the fact that Frontier still has not fully informed him of key details about the Data Breach's occurrence or the information stolen.

222. Moreover, since the Data Breach Plaintiff Retter has experienced suspicious spam calls and texts using his compromised Private Information, and believes this to be an attempt to secure additional information from or about him.

Plaintiff Joselyn Chiong

223. Plaintiff Joselyn Chiong is a former customer of Frontier. As a condition of receiving internet and/or cable products and services from Frontier, Plaintiff Chiong was required to supply Frontier with her Private Information, including her name, contact information, Social Security number, usage information, and other sensitive information.

224. Plaintiff Chiong greatly values her privacy and is very careful about sharing her sensitive Private Information. Plaintiff Chiong diligently protects her Private Information and stores documents with Private Information in a safe and secure location. She has never knowingly transmitted unencrypted Private Information over the internet or other unsecured source.

225. Plaintiff Chiong would not have provided her Private Information to Frontier had she known it would be kept using inadequate data security and vulnerable to a cyberattack.

226. At the time of the Data Breach—in or around April 2024—Frontier retained Plaintiff Chiong's Private Information in its network systems with inadequate data security, causing Plaintiff Chiong's Private Information to be accessed and exfiltrated by RansomHub in the Data Breach.

227. On or about June 6, 2024, Plaintiff Chiong received Frontier's Notice Letter informing that her Private Information was accessed and exposed to unauthorized hackers in the Data Breach. According to the Notice Letter, hackers acquired files containing Plaintiff Chiong's sensitive Private Information, including her name, date of birth, and Social Security number.

228. Plaintiff Chiong has made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Among other things, Plaintiff Chiong has already expended hours and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the present and future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing account statements and credit monitoring information, changing her account passwords, visiting her local bank to discuss protocols for protecting her accounts, and taking other protective and ameliorative steps in response to the Data Breach.

229. Plaintiff Chiong's Private Information compromised in the Data Breach has already been misused to commit identity theft and fraud. Specifically, since the Data Breach Plaintiff Chiong has experienced identity theft in the form of a credit check in her name that she did not authorize or recognize. Prior to this incident, Plaintiff Chiong to her knowledge had never been the

victim of identity theft or fraud.

230. Additionally, in June 2024, Plaintiff Chiong received notifications from her credit monitoring service alerting her that her Private Information was found on the dark web.

231. Plaintiff Chiong further anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Due to the Data Breach, Plaintiff Chiong is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

232. The risk of identity theft is impending and has materialized, as Plaintiff Chiong's and Class Members' Private Information was targeted, accessed, misused, and disseminated on the dark web by RansomHub, a notorious criminal organization.

233. The Data Breach has caused Plaintiff Chiong to suffer fear, anxiety, and stress, which has been compounded by the fact that Frontier still has not fully informed her of key details about the Data Breach's occurrence or the information stolen. Plaintiff Chiong fears that criminals will use her information to commit identity theft. Plaintiff Chiong has worked hard to build up her credit. As the primary earner for her family, Plaintiff Chiong is very distressed about the possibility that her credit could be negatively affected by misuse of her Private Information.

234. Moreover, since the Data Breach Plaintiff Chiong has experienced suspicious spam calls and solicitations using her compromised Private Information, and believes this to be an attempt to secure additional information from or about her.

Plaintiff Timothy Morgan

235. At the time of the Data Breach—in or around April 2024—Frontier retained Plaintiff Timothy Morgan's Private Information in its network systems with inadequate data security, causing Plaintiff Timothy Morgan's Private Information to be accessed and exfiltrated by

RansomHub in the Data Breach.

236. Plaintiff Timothy Morgan greatly values his privacy and is very careful about sharing his sensitive Private Information. Plaintiff Timothy Morgan diligently protects his Private Information and stores any documents containing Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

237. Plaintiff Timothy Morgan would not have provided his Private Information to Frontier had he known it would be kept using inadequate data security and vulnerable to a cyberattack.

238. On or about June 6, 2024, Plaintiff Timothy Morgan received Frontier's Notice Letter informing that his Private Information was accessed and exposed to unauthorized hackers in the Data Breach. According to the Notice Letter, hackers acquired files containing Plaintiff Timothy Morgan's sensitive Private Information, including his name, date of birth, and Social Security number.

239. Plaintiff Timothy Morgan has made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Among other things, Plaintiff Timothy Morgan has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including researching facts about the Data Breach, monitoring financial account and credit card activity, thoroughly reviewing financial account statements and credit card statements, and taking other protective and ameliorative steps. Plaintiff Timothy Morgan now monitors his financial and credit statements multiple times a week and has spent hours

dealing with the Data Breach, valuable time he otherwise would have spent on other activities.

240. Plaintiff Timothy Morgan further anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Due to the Data Breach, Plaintiff Timothy Morgan is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

241. The risk of identity theft is impending and has materialized, as Plaintiff Timothy Morgan's and Class Members' Private Information was targeted, accessed, misused, and disseminated on the dark web by RansomHub, a notorious criminal organization.

242. The Data Breach has caused Plaintiff Timothy Morgan to suffer fear, anxiety, and stress, particularly due to the invasion of his privacy and concern that he will be the victim of identity theft or suffer financial losses or damage to his credit, which has been compounded by the fact that Frontier still has not fully informed him of key details about the Data Breach's occurrence or the information stolen.

243. Moreover, since the Data Breach Plaintiff Timothy Morgan has experienced suspicious spam calls and texts using his compromised Private Information, and he believes this to be an attempt to secure additional information from or about him.

Plaintiff James Pratt II

244. Plaintiff James Pratt II is a current customer of Frontier. As a condition of receiving internet products and services from Frontier, Plaintiff Pratt was required to supply Frontier with his Private Information, including his name, contact information, Social Security number, usage information, and other sensitive information.

245. Plaintiff Pratt greatly values his privacy and is very careful about sharing his sensitive Private Information. Plaintiff Pratt diligently protects his Private Information and stores

any documents containing Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

246. Plaintiff Pratt would not have provided his Private Information to Frontier had he known it would be kept using inadequate data security and vulnerable to a cyberattack.

247. At the time of the Data Breach—in or around April 2024—Frontier retained Plaintiff Pratt's Private Information in its network systems with inadequate data security, causing Plaintiff Pratt's Private Information to be accessed and exfiltrated by RansomHub in the Data Breach.

248. On or about June 6, 2024, Plaintiff Pratt received Frontier's Notice Letter informing that his Private Information was accessed and exposed to unauthorized hackers in the Data Breach. According to the Notice Letter, hackers acquired files containing Plaintiff Pratt's sensitive Private Information, including his name, date of birth, and Social Security number.

249. Plaintiff Pratt has made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Among other things, Plaintiff Pratt has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing financial account statements and credit card statements, and taking other protective and ameliorative steps. Plaintiff Pratt now monitors his financial and credit statements multiple times a week and has spent hours dealing with the Data Breach, valuable time he otherwise would have spent on other activities.

250. Plaintiff Pratt's Private Information compromised in the Data Breach has already

been misused, as evidenced by notifications Plaintiff Pratt received since the Data Breach alerting that his home address had been found on the dark web, along with multiple spam calls Plaintiff has received since the Data Breach regarding fraudulent loans and requests for money from him.

251. Plaintiff Pratt further anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Due to the Data Breach, Plaintiff Pratt is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

252. The risk of identity theft is impending and has materialized, as Plaintiff Pratt's and Class Members' Private Information was targeted, accessed, misused, and disseminated on the dark web by RansomHub, a notorious criminal organization.

253. The Data Breach has caused Plaintiff Pratt to suffer fear, anxiety, and stress, particularly due to the invasion of his privacy and concern that he will be the victim of identity theft, which has been compounded by the fact that Frontier still has not fully informed him of key details about the Data Breach's occurrence or the information stolen.

254. Moreover, since the Data Breach Plaintiff Pratt has experienced suspicious spam calls and texts using his compromised Private Information, and believes this to be an attempt to secure additional information from or about him.

Plaintiff Seth Burton

255. Plaintiff Seth Burton is a former customer of Frontier. As a condition of receiving internet products and services from Frontier, Plaintiff Burton was required to supply Frontier with his Private Information, including his name, contact information, Social Security number, usage information, and other sensitive information.

256. Plaintiff Burton greatly values his privacy and is very careful about sharing his

sensitive Private Information. Plaintiff Burton diligently protects his Private Information and stores any documents containing Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

257. Plaintiff Burton would not have provided his Private Information to Frontier had he known it would be kept using inadequate data security and vulnerable to a cyberattack.

258. At the time of the Data Breach—in or around April 2024—Frontier retained Plaintiff Burton's Private Information in its network systems with inadequate data security, causing Plaintiff Burton's Private Information to be accessed and exfiltrated by RansomHub in the Data Breach.

259. On or about June 6, 2024, Plaintiff Burton received Frontier's Notice Letter informing that his Private Information was accessed and exposed to unauthorized hackers in the Data Breach. According to the Notice Letter, hackers acquired files containing Plaintiff Burton's sensitive Private Information, including his name, date of birth, and Social Security number.

260. Plaintiff Burton has made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Among other things, Plaintiff Burton has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing financial account statements and credit card statements, and taking other protective and ameliorative steps. Plaintiff Burton now monitors his financial and credit statements multiple times a week and has spent hours dealing with the Data Breach, valuable time he otherwise would have

spent on other activities.

261. Plaintiff Burton further anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Due to the Data Breach, Plaintiff Burton is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

262. The risk of identity theft is impending and has materialized, as Plaintiff Burton's and Class Members' Private Information was targeted, accessed, misused, and disseminated on the dark web by RansomHub, a notorious criminal organization.

263. The Data Breach has caused Plaintiff Burton to suffer fear, anxiety, and stress, particularly due to the invasion of his privacy and concern that he will be the victim of identity theft or suffer financial losses or damage to his credit, which has been compounded by the fact that Frontier still has not fully informed him of key details about the Data Breach's occurrence or the information stolen.

264. Moreover, since the Data Breach Plaintiff Burton has experienced suspicious spam calls and texts using his compromised Private Information, and believes this to be an attempt to secure additional information from or about him.

Plaintiff Lori Rusk

265. Plaintiff Lori Rusk is a former customer of Frontier. As a condition of receiving internet and/or cable products and services from Frontier, Plaintiff Rusk was required to supply Frontier with her Private Information, including her name, contact information, Social Security number, usage information, and other sensitive information.

266. Plaintiff Rusk greatly values her privacy and is very careful about sharing her sensitive Private Information. Plaintiff Rusk diligently protects her Private Information and stores

any documents containing Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

267. Plaintiff Rusk would not have provided her Private Information to Frontier had she known it would be kept using inadequate data security and vulnerable to a cyberattack.

268. At the time of the Data Breach—in or around April 2024—Frontier retained Plaintiff Rusk's Private Information in its network systems with inadequate data security, causing Plaintiff Rusk's Private Information to be accessed and exfiltrated by RansomHub in the Data Breach.

269. On or about June 6, 2024, Plaintiff Rusk received Frontier's Notice Letter informing that her Private Information was accessed and exposed to unauthorized hackers in the Data Breach. According to the Notice Letter, hackers acquired files containing Plaintiff Rusk's sensitive Private Information, including her name, date of birth, and Social Security number.

270. Plaintiff Rusk has made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Among other things, Plaintiff Rusk has already expended hours and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the present and future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing account statements and credit monitoring information, changing account passwords, and taking other protective and ameliorative steps.

271. Plaintiff Rusk's Private Information compromised in the Data Breach has already been misused to commit identity theft and fraud. Specifically, since the Data Breach Plaintiff Rusk

has experienced identity theft in the form of an unauthorized and unknown individual using her compromised Private Information in an attempt to open a fraudulent financial account in Plaintiff Rusk's name.

272. In addition, following the Data Breach Plaintiff Rusk was notified by her credit monitoring service that her Private Information had been found on the dark web.

273. Plaintiff Rusk further anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Due to the Data Breach, Plaintiff Rusk is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

274. The risk of identity theft is impending and has materialized, as Plaintiff Rusk's and Class Members' Private Information was targeted, accessed, misused, and disseminated on the dark web by RansomHub, a notorious criminal organization.

275. The Data Breach has caused Plaintiff Rusk to suffer fear, anxiety, and stress about her Private Information being in cybercriminals' hands and the increased risk of identity theft she now faces, which has been compounded by the fact that Frontier still has not fully informed her of key details about the Data Breach's occurrence or the information stolen.

276. Moreover, since the Data Breach Plaintiff Rusk has experienced suspicious spam calls and solicitations using her compromised Private Information, and believes this to be an attempt to secure additional information from or about her.

Plaintiff Gerald Wilson

277. Plaintiff Gerald Wilson is a former customer of Frontier. As a condition of receiving internet products and services from Frontier, Plaintiff Wilson was required to supply

Frontier with his Private Information, including his name, contact information, Social Security number, usage information, and other sensitive information.

278. Plaintiff Wilson greatly values his privacy and is very careful about sharing his sensitive Private Information. Plaintiff Wilson diligently protects his Private Information and stores any documents containing Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

279. Plaintiff Wilson would not have provided his Private Information to Frontier had he known it would be kept using inadequate data security and vulnerable to a cyberattack.

280. At the time of the Data Breach—in or around April 2024—Frontier retained Plaintiff Wilson's Private Information in its network systems with inadequate data security, causing Plaintiff Wilson's Private Information to be accessed and exfiltrated by RansomHub in the Data Breach.

281. On or about June 6, 2024, Plaintiff Wilson received Frontier's Notice Letter informing that his Private Information was accessed and exposed to unauthorized hackers in the Data Breach. According to the Notice Letter, hackers acquired files containing Plaintiff Wilson's sensitive Private Information, including his name, date of birth, and Social Security number.

282. Plaintiff Wilson has made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Among other things, Plaintiff Wilson has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly

reviewing financial account statements and credit card statements, and taking other protective and ameliorative steps. Plaintiff Wilson now monitors his financial and credit statements multiple times a week and has spent hours dealing with the Data Breach, valuable time he otherwise would have spent on other activities.

283. Plaintiff Wilson further anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Due to the Data Breach, Plaintiff Wilson is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

284. The risk of identity theft is impending and has materialized, as Plaintiff Wilson's and Class Members' Private Information was targeted, accessed, misused, and disseminated on the dark web by RansomHub, a notorious criminal organization.

285. The Data Breach has caused Plaintiff Wilson to suffer fear, anxiety, and stress, particularly due to the invasion of his privacy and concern that he will be the victim of identity theft or suffer financial losses or damage to his credit, which has been compounded by the fact that Frontier still has not fully informed him of key details about the Data Breach's occurrence or the information stolen.

286. Moreover, since the Data Breach Plaintiff Wilson has experienced suspicious spam calls and texts using his compromised Private Information, and believes this to be an attempt to secure additional information from or about him.

VI. CLASS ACTION ALLEGATIONS

287. Plaintiffs bring this nationwide class action on behalf of themselves and all others similarly situated pursuant to Federal Rule of Civil Procedure 23(b)(2), 23(b)(3), and 23(c)(4).

288. Plaintiffs propose the following nationwide class definition, subject to amendment based on information obtained through discovery:

> All persons in the United States whose Private Information was compromised in the Data Breach, including all persons who received a Notice Letter ("Nationwide Class").

289. Pursuant to Federal Rule of Civil Procedure 23(b)(2) and (b)(3), and (c)(4), as appropriate, Plaintiffs seek certification of state common law claims in the alternative to the nationwide claims, as well as statutory claims under state data breach and/or consumer protection statutes, on behalf of subclasses for residents of California, Connecticut, Florida, Illinois, New York, Ohio, and South Carolina (collectively, "State Subclasses") (for purposes of this Section VI, Nationwide Class and State Subclasses are referred to herein collectively"Classes").

290. Each State Subclass is defined as follows:

> California Subclass
>
> All residents of California whose Private Information was compromised in the Data Breach, including all California residents who received a Notice Letter.
>
> Connecticut Subclass
>
> All residents of Connecticut whose Private Information was compromised in the Data Breach, including all Connecticut residents who received a Notice Letter.
>
> Florida Subclass
>
> All residents of Florida whose Private Information was compromised in the Data Breach, including all Florida residents who received a Notice Letter.
>
> Illinois Subclass
>
> All residents of Illinois whose Private Information was compromised in the Data Breach, including all Illinois residents who received a Notice Letter.

New York Subclass

All residents of New York whose Private Information was compromised in the Data Breach, including all New York residents who received a Notice Letter.

Ohio Subclass

All residents of Ohio whose Private Information was compromised in the Data Breach, including all Ohio residents who received a Notice Letter.

South Carolina Subclass

All residents of South Carolina whose Private Information was compromised in the Data Breach, including all South Carolina residents who received a Notice Letter.

291. Excluded from the Classes are the following individuals and/or entities: Frontier and Frontier's parents, subsidiaries, affiliates, officers and directors, and any entity in which any Frontier has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

292. Plaintiffs reserve the right to modify or amend the definition of the proposed Classes before the Court determines whether certification is appropriate.

293. **Numerosity:** Each of the Classes is so numerous that joinder of all members is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, Frontier has reported that the Private Information of at least 750,000 individuals throughout the United States was compromised in the Data Breach. Upon information and belief, there are at least thousands of members in each State Subclass, making joinder of all members of the State Subclasses impractical.

294. **Commonality:** Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether Frontier unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' Private Information;

b. Whether and to what extent Frontier had a duty to protect the Private Information of Plaintiffs and Class Members;

c. Whether Frontier had a duty not to disclose the Private Information of Plaintiffs and Class Members to unauthorized third parties;

d. Whether Frontier had a duty not to use the Private Information of Plaintiffs and Class Members for non-business purposes;

e. Whether Frontier knew or should have known of the data security vulnerabilities that allowed the Data Breach to occur;

f. Whether Frontier knew or should have known of the risks to Plaintiffs' and Class Members' Private Information in its custody;

g. Whether Frontier failed to adequately safeguard the Private Information of Plaintiffs and Class Members;

h. Whether Frontier's data security systems prior to, during, and since the Data Breach complied with industry standards;

i. When Frontier actually learned of the Data Breach;

j. Whether Frontier adequately, promptly, and accurately informed Plaintiffs and Class Members of the Data Breach or that their Private Information had been compromised;

k. Whether Frontier violated data breach notification laws by failing to promptly notify Plaintiffs and Class Members that their Private Information had been compromised;

l. Whether Frontier conduct violated the FTC Act;

m. Whether Frontier failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;

n. Whether Frontier adequately addressed and fixed the vulnerabilities that permitted the Data Breach to occur;

o. Whether Frontier engaged in unfair, unlawful, or deceptive practice by failing to safeguard the Private Information of Plaintiffs and Class Members;

p. Whether Frontier engaged in unfair, unlawful, or deceptive practice by concealing and/or misrepresenting its data security processes and vulnerabilities;

q. Whether Frontier was unjustly enriched by failing to provide adequate security for Plaintiffs' and Class Members' Private Information;

r. Whether Plaintiffs and Class Members are entitled to actual, consequential, nominal, statutory, and/or punitive damages as a result of Frontier's wrongful conduct;

s. Whether Plaintiffs and Class Members are entitled to restitution as a result of Frontier's wrongful conduct; and

t. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm the Data Breach caused.

295. **Typicality:** As to the Classes, Plaintiffs' claims are typical of other Class Members' claims because Plaintiffs and Class Members were subject to the same unlawful conduct as alleged herein, and were damaged in the same way. Plaintiffs' Private Information was in Frontier's possession at the time of the Data Breach and was compromised due to the Data Breach. Plaintiffs' damages and injuries are akin to those of other Class Members and Plaintiffs seek relief consistent

with the relief of the Classes.

296. **Adequacy:** Plaintiffs are adequate representatives of the Classes because Plaintiffs are all members of the Nationwide Class and, respectively, members of the State Subclasses, and are committed to pursuing this matter against Frontier to obtain relief for the Classes. Plaintiffs have no conflicts of interest with the Classes. Plaintiffs' Counsel are competent and experienced in litigating class actions, including extensive experience in data breach and privacy litigation. Plaintiffs intend to vigorously prosecute this case and will fairly and adequately protect the interests of all the Classes.

297. **Superiority:** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to Plaintiffs and Class Members may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiffs and Class Members are relatively small compared to the burden and expense required to individually litigate their claims against Frontier, and thus, individual litigation to redress Frontier's wrongful conduct would be impracticable. Individual litigation by each Class Member would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

298. **Manageability:** The litigation of the class claims alleged herein is manageable. Frontier's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates there would be no significant manageability problems

with prosecuting this lawsuit as a class action. Adequate notice can be given to Class Members directly using information maintained in Frontier's records.

299. **Ascertainability:** All members of the proposed Classes are readily ascertainable. The Classes are defined by reference to objective criteria, and there is an administratively feasible mechanism to determine who fits within the Classes. Frontier has access to information regarding the individuals affected by the Data Breach, and has already provided notifications to some or all of those people. Using this information, the members of the Classes can be identified, and their contact information ascertained for purposes of providing notice.

300. **Particular Issues:** Particular issues are appropriate for certification under Rule 23(c)(4) 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 the following:

a. Whether Frontier owed a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

b. Whether Frontier breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

c. Whether Frontier failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether an implied contract existed between Frontier on the one hand, and Plaintiffs and Class Members on the other, and the terms of that implied contract;

e. Whether Frontier breached the implied contract;

f. Whether Frontier adequately and accurately informed Plaintiffs and Class Members their Private Information had been compromised;

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

h. Whether Frontier engaged in unfair, unlawful, or deceptive practices by misrepresenting its data security processes and vulnerabilities;

i. Whether Frontier engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiffs and Class Members; and

j. Whether Class Members are entitled to actual, consequential, statutory, and/or nominal damages, and/or injunctive relief due to Frontier's wrongful conduct.

301. **Policies Generally Applicable to the Classes:** Finally, class certification is also appropriate under Rule 23(b)(2) and (c). Each of the Classes are also appropriate for certification because Defendants have 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 Class Members and making final injunctive relief appropriate with respect to each of the Classes as a whole. Defendants' policies challenged herein apply to and affect Class Members uniformly, and Plaintiffs' challenge of these policies hinges on Defendants' conduct with respect to the Classes as a whole, not on facts or law applicable only to Plaintiffs.

302. Frontier, through uniform conduct, acted or refused to act on grounds generally applicable to the Classes as a whole, making injunctive and declaratory relief appropriate to the Classes as a whole, including without limitation the following:

a. Ordering Frontier to provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

b. Ordering that, to comply with Frontier explicit or implicit contractual obligations and

duties of care, Frontier must implement and maintain reasonable security and monitoring measures, including, but not limited to the following:

(i) prohibiting Frontier from engaging in the wrongful and unlawful acts alleged herein;

(ii) requiring Frontier to protect, including through encryption, all data collected through the course of business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

(iii) requiring Frontier to delete and purge the Private Information of Plaintiffs and Class Members unless it can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

(iv) requiring Frontier to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiffs' and Class Members' Private Information;

(v) requiring Frontier to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests, and audits on Frontier's systems on a periodic basis;

(vi) prohibiting Frontier from maintaining Private Information on a cloud-based database until proper safeguards and processes are implemented;

(vii) requiring Frontier to segment data by creating firewalls and access controls so that, if one area of its network is compromised, hackers cannot gain access to other portions of Frontier's systems;

(viii) requiring Frontier to conduct regular database scanning and securing checks;

(ix) requiring Frontier to monitor ingress and egress of all network traffic;

(x) requiring Frontier to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling Private Information, as well as protecting the Private Information of Plaintiffs and Class Members;

(xi) requiring Frontier to implement, maintain, review, and revise as necessary a threat management program to appropriately monitor its networks for internal and external threats, and assess whether monitoring tools are properly configured, tested, and updated;

(xii) requiring Frontier to meaningfully educate all Class Members about the threats that they because of the loss of their confidential Private Information to third parties, as well as the steps affected individuals must take to protect themselves; and

(xiii) Incidental retrospective relief, including but not limited to restitution.

VII. CAUSES OF ACTION

COUNT I: NEGLIGENCE/NEGLIGENCE *PER SE*
(On behalf of Plaintiffs and the Nationwide Class, or alternatively, on behalf of the State Subclasses)

303. Plaintiffs re-allege and incorporate by reference paragraphs 1 through 302 above as if fully set forth herein.

304. Frontier required Plaintiffs and Class Members to submit sensitive, confidential Private Information to Frontier as a condition of receiving internet and/or television products and services from Frontier.

305. Plaintiffs and Class Members provided their Private Information to Frontier, including their names, Social Security numbers, dates of birth, usage information, financial information, and other sensitive data.

306. Frontier had full knowledge of the sensitivity of the Private Information to which it was entrusted, and the types of harm that Plaintiffs and Class Members could and would suffer if the Private Information was wrongfully disclosed to unauthorized persons.

307. Frontier owed a duty to Plaintiffs and each Class Member to exercise reasonable care in holding, safeguarding, and protecting the Private Information it collected from them.

308. Plaintiffs and Class Members were the foreseeable victims of any inadequate data safety and security practices by Frontier.

309. Plaintiffs and the Class Members had no ability to protect their Private Information in Frontier's possession.

310. By collecting, transmitting, and storing Plaintiffs' and Class Members' Private Information Frontier owed Plaintiffs and Class Members a duty of care to use reasonable means to secure and safeguard their Private Information, to prevent the information's unauthorized disclosure, and to safeguard it from theft or exfiltration to cybercriminals. Frontier's duty included the responsibility to implement processes by which it could detect and identify malicious activity or unauthorized access on its networks or servers.

311. Frontier owed a duty of care to Plaintiffs and the Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that controls for its networks, servers, and systems, and the personnel responsible for them, adequately protected Plaintiff's and Class Members' Private Information. This duty included the responsibility to train Frontier employees to recognize and prevent attempts to gain initial

unauthorized access through common techniques like phishing.

312. Frontier's duty to use reasonable security measures arose because of the special relationship that existed between it and its customers, which is recognized by laws and regulations including but not limited to the FTC Act, as well as the common law. Frontier was able to ensure its network servers and systems were sufficiently protected against the foreseeable harm a data breach would cause Plaintiffs and Class Members, yet it failed to do so.

313. In addition, Frontier had a duty to employ reasonable security measures under Section 5 of the FTC Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

314. Pursuant to the FTC Act, 15 U.S.C. § 45 *et seq.*, Frontier had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

315. Frontier breached its duty to Plaintiffs and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

316. The injuries to Plaintiffs and Class Members resulting from the Data Breach were directly and indirectly caused by Frontier's violation of the FTC Act.

317. Plaintiffs and Class Members are within the class of persons the FTC Act is intended to protect.

318. The type of harm that resulted from the Data Breach was the type of harm the FTC Act is intended to guard against.

319. Frontier's failure to comply with the FTC Act constitutes negligence *per se.*

320. Frontier's duty to use reasonable care in protecting Plaintiffs' and Class Members' confidential Private Information in its possession arose not only because of the statutes and regulations described above, but also because Frontier is bound by industry standards to reasonably protect such Private Information.

321. Frontier breached its duties of care, and was grossly negligent, by acts of omission or commission, including by failing to use reasonable measures or even minimally reasonable measures to protect the Plaintiffs' and Class Members' Private Information from unauthorized disclosure in this Data Breach.

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

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

b. Maintaining and/or transmitting Plaintiffs' and Class Members' Private Information in unencrypted and identifiable form;

c. Failing to implement data security measures, like adequate MFA for as many systems as possible, to safeguard against known techniques for initial unauthorized access to network servers and systems;

d. Failing to adequately train employees on proper cybersecurity protocols;

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

f. Failure to periodically ensure that their network system had plans in place to maintain reasonable data security safeguards;

g. Allowing unauthorized access to Plaintiffs' and Class Members' Private Information; and

h. Failing to timely or adequately notify Plaintiffs and Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

323. But for Frontier's wrongful and negligent breaches of its duties owed to Plaintiffs and Class Members, their Private Information would not have been compromised because the malicious activity would have been identified and stopped before RansomHub had a chance to inventory Frontier's digital assets, stage them, and then exfiltrate them.

324. It was foreseeable that Frontier's failures to use reasonable measures to protect Plaintiffs' and Class Members' Private Information would result in injury to Plaintiffs and Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in Frontier's industry.

325. It was therefore foreseeable that the failure to adequately safeguard Plaintiffs' and Class Members' Private Information would cause them one or more types of injuries.

326. As a direct and proximate result of Frontier's negligence, Plaintiffs and Class Members have suffered and will suffer injuries, including but not limited to (a) invasion of privacy; (b) lost or diminished value of their Private Information; (c) actual identity theft, or the imminent and substantial risk of identity theft or fraud; (d) out-of-pocket and lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (e) loss of benefit of the bargain; (f) anxiety and emotional harm due to their Private Information's disclosure to cybercriminals; and (g) the continued and certainly increased risk to their Private Information, which remains in Frontier's possession and is subject to further unauthorized disclosures so long as Frontier fails to undertake appropriate and adequate measures to protect it.

327. Plaintiffs and Class Members are entitled to damages, including compensatory, consequential, punitive, and nominal damages, in an amount to be proven at trial.

328. Plaintiffs and Class Members are also entitled to injunctive relief requiring Frontier to (a) strengthen its data security systems and monitoring procedures; (b) submit to future annual audits of those systems and monitoring procedures; and (c) provide adequate and lifetime credit monitoring to Plaintiffs and all Class Members.

COUNT II: BREACH OF EXPRESS CONTRACT
(On behalf of Plaintiffs and the Nationwide Class, or alternatively, on behalf of the State Subclasses)

329. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 302 above as if fully set forth herein.

330. Plaintiffs and Class Members entered into valid and enforceable express contracts with Frontier, under which Plaintiffs and Class Members agreed to provide their Private Information to Frontier, and Frontier agreed to provide Plaintiffs and Class Members internet and/or television products and services and expressly agreed to protect Plaintiffs' and Class members' Private Information.

331. To the extent Frontier's obligation to protect Plaintiffs' and Class Members' Private Information was not explicit in those express contracts, the express contracts included implied terms requiring Frontier to implement data security adequate to safeguard and protect the confidentiality of Plaintiffs' and Class Members' Private Information, including in accordance with trade regulations, federal, state and local laws, and industry standards.

332. No Plaintiff or Class Member would have entered into these express contracts with Frontier without understanding that their Private Information would be safeguarded and protected. Stated otherwise, data security was an essential implied term of the parties' express contracts.

333. A meeting of the minds occurred, as Plaintiffs and Class Members agreed, among other things, to provide their Private Information in exchange for Frontier's agreement to protect the confidentiality of that Private Information.

334. The protection of Plaintiffs' and Class Members' Private Information were material aspects of Plaintiffs' and Class Members' contracts with Frontier.

335. Frontier's promises and representations described above relating to industry practices, and about Frontier's purported concern about its clients' privacy rights became terms of the contracts between Frontier and its clients, including Plaintiffs and Class Members. Frontier breached these promises by failing to comply with reasonable industry standards.

336. Plaintiffs and Class Members read, reviewed, and/or relied on statements made by or provided by Frontier and/or otherwise understood that Frontier would protect its customers' Private Information if that information were provided to Frontier.

337. Plaintiffs and Class Members fully performed their obligations under the express contract with Frontier; however, Frontier did not.

338. As a result of Frontier's breach of the terms of the express contracts with Plaintiffs and Class Members, Plaintiffs and Class Members have suffered and will suffer injuries, including but not limited to (a) invasion of privacy; (b) lost or diminished value of their Private Information; (c) actual identity theft, or the imminent and substantial risk of identity theft or fraud; (d) out-of-pocket and lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (e) loss of benefit of the bargain; (f) anxiety and emotional harm due to their Private Information's disclosure to cybercriminals; and (g) the continued and certainly increased risk to their Private Information, which remains in Frontier's possession and is subject to further unauthorized disclosures so long as Frontier fails to

undertake appropriate and adequate measures to protect it.

339. Plaintiffs and Class members are therefore entitled to damages, including restitution, disgorgement, nominal damages, declaratory and injunctive relief, and attorney fees, costs, and expenses.

COUNT III: BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiffs and the Nationwide Class, or alternatively, on behalf of the State Subclasses)

340. Plaintiffs re-allege and incorporate by reference paragraphs 1 through 302 above as if fully set forth herein.

341. Frontier required Plaintiffs and Class Members to provide and entrust their Private Information to Frontier as a condition of and in exchange for receiving internet and/or cable products and services from Frontier.

342. When Plaintiffs and Class Members provided their Private Information to Frontier, they entered into implied contracts with Frontier pursuant to which Frontier agreed to safeguard and protect such Private Information and to timely and accurately notify Plaintiffs and Class Members if and when their Private Information was breached and compromised.

343. Specifically, Plaintiffs and Class Members entered into valid and enforceable implied contracts with Frontier when they agreed to provide their Private Information and/or payment to Frontier.

344. The valid and enforceable implied contracts that Plaintiffs and Class Members entered into with Frontier included Frontier's promises to protect Private Information it collected from Plaintiffs and Class Members, or created on its own, from unauthorized disclosures. Plaintiffs and Class Members provided this Private Information in reliance on Frontier's promises.

345. The valid and enforceable implied contracts that Plaintiffs and Class Members entered into with Frontier included Frontier's promises to protect Private Information it collected from Plaintiffs and Class Members, or created on its own, from unauthorized disclosures. Plaintiffs and Class Members provided this Private Information in reliance on Frontier's promises, including those in Frontier's Privacy Policy.

346. Under the implied contracts, Frontier promised and was obligated to (a) provide internet and/or cable products and services to Plaintiffs and Class Members; and (b) protect Plaintiffs' and Class Members' Private Information provided to obtain such products and services and/or created in connection therewith. In exchange, Plaintiffs and Class Members agreed to provide Frontier with payment and their Private Information.

347. Frontier promised and warranted to Plaintiffs and Class Members, including through its public-facing privacy documents identified *supra*, to maintain the privacy and confidentiality of the Private Information it collected from Plaintiffs and Class Members and to keep such information safeguarded against unauthorized access and disclosure.

348. Frontier's adequate protection of Plaintiffs' and Class Members' Private Information was a material aspect of these implied contracts with Frontier.

349. Frontier solicited and invited Plaintiffs and Class Members to provide their Private Information as part of Frontier's regular business practices. Plaintiffs and Class Members accepted Frontier's offers and provided their Private Information to Frontier.

350. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Frontier's data security practices complied with industry standards and relevant laws and regulations, including the FTC Act, as well as industry standards.

351. Plaintiffs and Class Members who contracted with Frontier for internet and/or

television products and services and provided their Private Information to Frontier reasonably believed and expected that Frontier would adequately employ adequate data security to protect that Private Information.

352. A meeting of the minds occurred when Plaintiffs and Class Members agreed to, and did, provide their Private Information to Frontier and agreed Frontier would receive payment for, amongst other things, the protection of their Private Information.

353. Plaintiffs and Class Members performed their obligations under the contracts when they provided their Private Information and/or payment to Frontier.

354. Frontier materially breached its contractual obligations to protect the Private Information they required Plaintiffs and Class Members to provide when that Private Information was unauthorizedly disclosed in the Data Breach due to Frontier's inadequate data security measures and procedures.

355. Frontier materially breached its contractual obligations to deal in good faith with Plaintiffs and Class Members when it failed to take adequate precautions to prevent the Data Breach and failed to promptly notify Plaintiffs and Class Members of the Data Breach.

356. Frontier materially breached the terms of their implied contracts, including but not limited to by failing to comply with industry standards or the standards of conduct embodied in statutes like Section 5 of the FTC Act, by failing to otherwise protect Plaintiffs' and Class Members' Private Information, as set forth *supra*.

357. The Data Breach was a reasonably foreseeable consequence of Frontier's breaches of these implied contracts with Plaintiffs and Class Members.

358. As a result of Frontier's failures to fulfill the data security protections promised in these contracts, Plaintiffs and Class Members did not receive the full benefit of their bargains with

Frontier, and instead received products and services of a diminished value compared to that described in the implied contracts. Plaintiffs and Class Members were therefore damaged in an amount at least equal to the difference in the value of the services with data security protection they paid for and that which they received.

359. Had Frontier disclosed that its data security procedures were inadequate or that it did not adhere to industry standards for cybersecurity, neither Plaintiffs, Class Members, nor any reasonable person would have contracted with Frontier.

360. Plaintiffs and Class Members would not have provided and entrusted their Private Information to Frontier in the absence of the implied contracts between them and Frontier.

361. Frontier breached the implied contracts it made with Plaintiffs and Class Members by failing to safeguard and protect their Private Information and by failing to provide timely or adequate notice that their Private Information was compromised in and due to the Data Breach.

362. As a direct and proximate result of Frontier's breach of its implied contracts with Plaintiffs and Class Members and the attendant Data Breach, Plaintiffs and Class Members have suffered injuries and damages as set forth herein and have been irreparably harmed, as well as suffering and the loss of the benefit of the bargain they struck with Frontier.

363. Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

COUNT IV: INVASION OF PRIVACY/INSTRUSION UPON SECLUSION
(On behalf of Plaintiffs and the Nationwide Class, or alternatively, on behalf of the State Subclasses)

364. Plaintiffs re-allege and incorporate by reference paragraphs 1 through 302 above as if fully set forth herein.

365. Plaintiffs and Class Members had a legitimate expectation of privacy to their Private

Information and were entitled to Frontier's protection of this Private Information in its possession against disclosure to unauthorized third parties.

366. Frontier owed a duty to its customers, including Plaintiffs and Class Members, to keep their Private Information confidential and secure.

367. Frontier failed to protect Plaintiffs' and Class Members' Private Information and instead exposed it to unauthorized persons, a notorious ransomware group, which has already made the Private Information publicly available and disseminated it to thousands of people, including through publishing the data on its dark web leak site, where cybercriminals go to find their next identity theft and extortion victims.

368. Frontier allowed unauthorized third parties access to and examination of the Private Information of Plaintiffs and Class Members, by way of Frontier's failure to protect the Private Information through reasonable data security measures.

369. The unauthorized release to, custody of, and examination by unauthorized third parties of the Private Information of Plaintiffs and Class Members is highly offensive to a reasonable person and represents an intrusion upon Plaintiffs' and Class Members' seclusion as well as a public disclosure of private facts.

370. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiffs and Class Members disclosed their Private Information to Frontier as a condition of and in exchange for receiving internet and/or television products and services, but privately with an intention that the Private Information would be kept confidential and protected from unauthorized disclosure. Plaintiffs and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

371. Subsequent to the intrusion, Frontier permitted Plaintiffs' and Class Members' data

to be published online to countless cybercriminals whose mission is to misuse such information, including through identity theft and extortion.

372. The Data Breach constitutes an intentional or reckless interference by Frontier with Plaintiffs' and Class Members' interests in solitude or seclusion, as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

373. Frontier acted with a knowing state of mind when it permitted the Data Breach to occur, because it had actual knowledge that its information security practices were inadequate and insufficient to protect Plaintiffs' and Class Members' Private Information from unauthorized disclosure.

374. Frontier acted with reckless disregard for Plaintiffs' and Class Members' privacy when it allowed improper access to its systems containing Plaintiffs' and Class Members' Private Information without protecting said data from the unauthorized disclosure, or even encrypting such information.

375. Frontier was aware of the potential of a data breach and failed to adequately safeguard its network systems or implement appropriate policies to prevent the unauthorized release of Plaintiffs' and Class Members' Private Information to cybercriminals.

376. Because Frontier acted with this knowing state of mind, it had notice and knew that its inadequate and insufficient information security practices would cause injury and harm to Plaintiffs and Class Members.

377. As a direct and proximate result of Frontier's acts and omissions set forth above, Plaintiffs' and Class Members' Private Information was disclosed to third parties without authorization, causing Plaintiffs and Class Members to suffer injuries and damages including, without limitation, (a) invasion of privacy; (b) lost or diminished value of their Private Information;

(c) out-of-pocket and lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (d) loss of benefit of the bargain; and (e) the continued and certainly increased risk to their Private Information, which remains in Frontier's possession in unencrypted form and subject to further unauthorized disclosures, so long as Frontier fails to undertake appropriate and adequate measures to protect it.

378. Unless and until enjoined and restrained by order of this Court, Frontier's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and Class Members in that the Private Information maintained by Frontier can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiffs and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiffs and Class Members.

COUNT V: CALIFORNIA CONSUMER PRIVACY ACT
Cal. Civ. Code § 1798.100, *et seq.* ("CCPA")
(On Behalf of Plaintiffs Carolus, Graham, Miller, Lauren Morgan, Muto, and Terrell and the California Subclass)

379. Plaintiffs Carolus, Graham, Miller, Lauren Morgan, Muto, and Terrell (for purposes of this count, "Plaintiffs") re-allege and incorporate by reference paragraphs 1–211 and 287–302 above as if fully set forth herein.

380. At all relevant times, Frontier has done business in the State of California and collected the PII of California residents, including Plaintiffs' and California Subclass members' Private Information.

381. The CCPA imposes a duty on entities that receive California residents' PII to implement and maintain reasonably security procedures and practices as appropriate given the nature of the sensitive information.

382. Under the CCPA, a business's "collection, use, retention, and sharing of a consumer's personal information" shall be reasonably necessary and proportionate to achieve the purposes for which the information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes. Cal. Civ. Code § 1798.100(c).

383. Further, under the CCPA, "[a] business that collects a consumer's personal information shall implement reasonable security procedures and practices appropriate to the nature of the personal information to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure." Cal. Civ. Code § 1798.100(e); *see also* § 1798.81.5.

384. Pursuant to the CCPA, any individual whose nonencrypted and nonredacted personal information is accessed, exfiltrated, stolen, or disclosed as a result of the business's violation of its duty to collect, use, retain, and share personal information about a consumer only in manners compatible with the business's purpose in collecting such information are entitled to damages, including statutory damages. Cal. Civ. Code § 1798.150.

385. Plaintiffs' and California Subclass members' Private Information compromised in the Data Breach is "personal information about a consumer" as used in the CCPA. Cal. Civ. Code §§ 1798.80(e), 1798.150(a).

386. Frontier collected Plaintiffs' and California Subclass members' Private Information for the purpose of contracting with Plaintiffs and California Subclass members, furnishing products and services to Plaintiffs and California Subclass members, and billing Plaintiffs and California Subclass members.

387. When the Data Breach occurred, Frontier maintained Plaintiffs' and California Subclass members' Private Information on its network server(s) and/or systems in unencrypted and

unredacted form.

388. When the Data Breach occurred, Frontier did not have reasonable security procedures and practices appropriate to the nature of the Private Information it collected to protect such Private Information from unauthorized or illegal access, destruction, use, or disclosure.

389. Exposure of Plaintiffs' and California Subclass members' Private Information to unauthorized cybercriminals, as in this Data Breach, is incompatible with Frontier's purpose in collecting or processing such information.

390. Frontier violated the CCPA by failing to implement data security measures as reasonably necessary and proportionate to protect Plaintiffs' and California Subclass members' Private Information it collected and processed.

391. Frontier further violated the CCPA by failing to use Plaintiffs' and California Subclass members' Private Information in a manner that is reasonably necessary and proportionate to achieve the purposes for which such Private Information was collected.

392. As a direct and proximate result of Frontier's failure to implement reasonably necessary and proportionate data security measures as required by the CCPA, Plaintiffs' and California Subclass members' unencrypted and unredacted Private Information was wrongfully disclosed to a notorious cybercriminal group in the Data Breach, then published and disseminated on the dark web, causing Plaintiffs' and Class Members' injuries and damages as set forth herein.

393. On or before August 8, 2024, Frontier received notice of this CCPA claim from Plaintiffs Muto, Graham, Carolus, and Lauren Morgan on behalf of the California Subclass. To date, Frontier has failed to cure its CCPA violations.

394. Plaintiffs and the California Subclass are entitled to damages, including statutory damages, due to Frontier's CCPA violations. Cal. Civ. Code § 1798.150.

COUNT VI: CONNECTICUT UNFAIR TRADE PRACTICES ACT
Conn. Gen. Stat. § 42-110b ("CUTPA")
(On Behalf of Plaintiff Retter and the Connecticut Subclass)

395. Plaintiff Retter (for purposes of this count, "Plaintiff") re-alleges and incorporates by reference paragraphs 1–146, 212–222, and 287–302 above as if fully set forth herein.

396. CUTPA prohibits unfair or deceptive acts or practices in the conduct of any trade or commerce. Conn. Gen. Stat. § 42-110b(a).

397. Frontier engaged in trade or commerce as used in CUTPA because it offered for sale and distributed services and things of value in Connecticut, affecting Connecticut residents.

398. Plaintiff, Connecticut Subclass members, and Frontier are all "persons" as defined and used in CUTPA.

399. Plaintiff and Connecticut Subclass members purchased services and/or things of value from Frontier for personal and/or family purposes.

400. Frontier engaged in unfair or deceptive acts and practices in trade or commerce that affected Connecticut residents, in violation of CUTPA, by representing that it had implemented reasonable and adequate data security processes and procedures to protect Plaintiff and Connecticut Subclass members' Private Information, when in reality, Frontier's data security processes and procedures were deficient and left Plaintiff and Connecticut Subclass members' Private Information vulnerable to the Data Breach.

401. Frontier further engaged in unfair or deceptive acts and practices in the conduct of trade or commerce in Connecticut, in violation of CUTPA, by representing that it had data security processes and procedures that complied with the FTC Act and industry standards to protect Plaintiff and Connecticut Subclass members' Private Information, when in reality, Frontier's data security processes and procedures did not comply with the FTC Act or industry standards and left Plaintiff

and Connecticut Subclass members' Private Information vulnerable to the Data Breach.

402. Frontier's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Frontier's data security measures and its ability to protect the confidentiality of consumers' Private Information.

403. Frontier acted intentionally, knowingly, and maliciously to violate the CUTPA, and recklessly disregarded Plaintiff and Connecticut Subclass members' rights.

404. As a direct and proximate result of Frontier's deceptive and unlawful acts and practices and violations of CUTPA, Plaintiff and Connecticut Subclass members have suffered and will continue to suffer ascertainable losses of money or property, including but not limited to fraud and identity theft; time and expenses related to monitoring their accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Private Information; overpayment for Frontier's services; and the cost of identity protection services made necessary by the Data Breach.

405. Pursuant to CUTPA, Plaintiff and Connecticut Subclass members are entitled to recover actual damages, reasonable attorneys' fees, and costs due to Frontier's CUTPA violations.

406. Plaintiff, individually and on behalf the Connecticut Subclass, further seeks punitive damages and injunctive/equitable relief, as appropriate, due to Frontier's CUTPA violations.

COUNT VII: FLORIDA UNFAIR AND DECEPTIVE TRADE PRACTICES ACT
Fla. Stat. § 501.201 *et seq.* ("FDUPTA")
(On Behalf of Plaintiffs Chiong and Timothy Morgan and the Florida Subclass)

407. Plaintiffs Chiong and Timothy Morgan (for purposes of this count, "Plaintiffs") re-allege and incorporate by reference paragraphs 1–146, 223–243, and 287–302 above as if fully set forth herein.

408. FDUPTA, Fla. Stat. § 501.201 *et seq.*, is expressly intended to protect consumers like Plaintiffs and Florida Subclass members from unfair or deceptive trade practices.

409. Plaintiffs and Florida Subclass members have a vested interest in the privacy, security and integrity of their Private Information, and therefore, this interest is a "thing of value" as contemplated by FUDTPA.

410. Frontier is a "person" within the meaning of FUDTPA and, at all pertinent times, was subject to FDUPTA's requirements and proscriptions with respect to all of Frontier's business and trade practices described herein.

411. Frontier engaged in unfair and deceptive trade practices by creating a false expectation of privacy to Florida consumers, including Plaintiffs and Florida Subclass members, through representations and promises that their Private Information in Frontier's custody will be kept safe through adequate and reasonable data security measures that comply with the FTC Act and industry standards, while in reality Frontier failed to take commercially reasonable steps to protect the Private Information entrusted to it.

412. Frontier engaged in deceptive and unfair acts and practices, misrepresentations, and the concealment and omission of material facts in connection with the sale and advertisement of services in violation of FDUTPA, including without limitation by the following:

a. Failing to maintain adequate data security to keep Plaintiffs' and Florida Subclass members' Private Information from being accessed and taken by cybercriminals;

b. Failing to comply with applicable state and federal laws and industry standards pertaining to data security, including the FTC Act;

c. Failing to disclose and omitting materials facts to Plaintiffs and Florida Subclass members regarding Frontier's lack of adequate data security and inability or

unwillingness to properly secure and protect Plaintiffs' and Florida Subclass members' Private Information;

d. Failing to disclose and/or omitting material facts to Plaintiffs and Florida Subclass members about Frontier's failure to comply with federal and state laws on the privacy and security of Plaintiffs' and Florida Subclass members' Private Information; and

e. Failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiffs' and Florida Subclass members' Private Information from further unauthorized disclosure, release, breaches, and theft.

413. These actions also constitute deceptive and unfair acts or practices because Frontier knew the facts about its inadequate data security and failure to comply with applicable state and federal laws and industry standards would be unknown to and not easily discoverable by Plaintiffs and Florida Subclass members, and would erase the false impression of adequate security for their Private Information if known.

414. But for Frontier's unfair acts and practices and deceptive misrepresentations and omissions, Plaintiffs and Florida Subclass members would have known the truth about Frontier's inadequate data security measures and would not have provided their Private Information to, or entered into transactions with, Frontier.

415. Frontier's wrongful practices were and are injurious to the public because they were and are part of its generalized course of conduct that applied to the Florida Subclass as a whole. Plaintiffs, Florida Subclass members, and the public have been adversely affected by Frontier's conduct and the public was and is at risk as a result thereof.

416. Plaintiffs and Florida Subclass members are consumers "likely to be damaged" by Frontier's ongoing deceptive trade practices.

417. Frontier's unfair conduct as described herein was directed and emanated from its Florida business operations to the detriment of Plaintiffs and Florida Subclass members in Florida.

418. Plaintiffs and Florida Subclass members have standing to pursue this claim because as a direct and proximate result of Frontier's violations of FDUTPA, Plaintiffs and Florida Subclass members have been "aggrieved" by a violation of FDUTPA and bring this action to obtain a declaratory judgment that Frontier's acts or practices violate FDUTPA. *See* Fla. Stat. § 501.211(a).

419. Plaintiffs and Florida Subclass members also have standing to pursue this claim because, as a direct result of Frontier's knowing violations of FDUTPA, Plaintiffs and Florida Subclass members are at a substantial present and imminent risk of identity theft. Frontier still possesses Plaintiffs' and Florida Subclass members' Private Information, which has already been accessed by unauthorized third parties, evidencing of a substantial and imminent risk of future identity theft for Plaintiffs and the Florida Subclass.

420. Plaintiffs and Florida Subclass members are entitled to injunctive relief to protect them from the substantial and imminent risk of future identity theft, including, but not limited to the following:

a. ordering that Frontier engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Frontier's systems on a periodic basis, and ordering prompt correction of any problems or issues detected by such third-party security auditors;

b. ordering that Frontier engage third-party security auditors and internal personnel to run automated security monitoring;

c. ordering that Frontier audit, test, and train security personnel regarding any new or modified procedures;

d. ordering that Frontier segment data by, among other things, creating firewalls and access controls so that if one area of a network system is compromised, hackers cannot gain access to other portions of the system;

e. ordering that Frontier purge, delete, and destroy Private Information not necessary for its provisions of services in a reasonably secure manner;

f. ordering that Frontier conduct regular database scans and security checks;

g. ordering that Frontier routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. ordering Frontier to meaningfully educate individuals about the threats they face as a result of the loss of their financial and Private Information to third parties, as well as the steps victims should take to protect themselves.

421. Plaintiffs bring this action individually and on behalf of the Florida Subclass for the relief requested above and for the public benefit to promote the public interests in the provision of truthful, fair information to allow consumers to make informed purchasing decisions and to protect Plaintiffs, the Florida Subclass, and the public from Frontier's unfair methods of competition and unfair, unconscionable, and unlawful practices. Frontier's wrongful conduct as alleged herein has had widespread impact on the public at large.

422. The above unfair, unconscionable, and unlawful practices and acts by Frontier were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiffs and Florida Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

423. Frontier's actions and inactions in the unfair, unconscionable, and unlawful

practices described herein were negligent, knowing and willful, and/or wanton and reckless.

424. Plaintiffs and Florida Subclass members seek relief under FDUTPA, Fla. Stat. §§ 501.201, *et seq*., including, but not limited to, a declaratory judgment that Frontier's actions and/or practices violate FDUTPA.

425. Under FDUPTA, Plaintiffs and Florida Subclass members are entitled to preliminary and permanent injunctive relief without proof of monetary damage, loss of profits, or intent to deceive. Plaintiffs and Florida Subclass members seek equitable relief and to enjoin Frontier on terms that the Court considers appropriate.

426. Frontier's conduct in violation of FDUPTA caused and continues to cause substantial injury to Plaintiff and Florida Subclass members. Unless preliminary and permanent injunctive relief is granted, Plaintiffs and Florida Subclass members will suffer harm. Plaintiffs and Florida Subclass members do not have an adequate remedy at law, and the balance of the equities weighs in favor of Plaintiffs and Florida Subclass members, the victims of Frontier's unfair and deceptive conduct.

427. At all material times, Frontier's unfair and deceptive trade practices were willful within the meaning of FUDTPA, and accordingly, Plaintiffs and Florida Subclass members are entitled to an award of attorneys' fees, costs and other recoverable expenses of litigation

COUNT VIII: ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT 815 Ill. Comp. Stat. § 505/1, *et seq*. ("ICFA")
(On Behalf of Plaintiff Pratt and the Illinois Subclass)

428. Plaintiff Pratt (for the purposes of this count, "Plaintiff") re-alleges and incorporates by reference paragraphs 1–146, 244–254, and 287–302 above as if fully set forth herein.

429. Plaintiff and the Illinois Subclass are "consumers" as defined in 815 Ill. Comp. Stat. § 505/1(e).

430. Frontier, Plaintiff, and Illinois Subclass members are "persons" as defined in 815 Ill. Comp. Stat. § 505/1(c).

431. Frontier engaged in "trade" or "commerce," including the provision of services, as defined under 815 Ill. Comp. Stat. § 505/1(f). Frontier also engages in the sale of "merchandise" (including services) as defined by 815 Ill. Comp. Stat. § 505/1(b) and (d).

432. Pursuant to Frontier's trade or commerce, Frontier disclosed Plaintiff's and Illinois Subclass members' Private Information to unauthorized parties in the Data Breach.

433. Frontier engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment and omission of material facts in connection with the sale and advertisement of its services in violation of the ICFA, including by (a) failing to maintain and/or ensure that adequate data security was used to keep Plaintiff's and Illinois Subclass members' sensitive Private Information from being accessed or stolen by cybercriminals, (b) failing to comply with applicable state and federal laws and industry standards pertaining to data security, including the FTC Act; (c) failing to disclose or omitting material facts to Plaintiff and Illinois Subclass members regarding Frontier's lack of adequate data security and inability and/or unwillingness to properly secure and protect the Private Information of Plaintiff and Illinois Subclass members; (d) failing to take proper action following the Data Breach to notify Plaintiff and Illinois Subclass members or enact adequate privacy and security measures to protect Plaintiff's and Illinois Subclass members' Private Information from further unauthorized disclosure, release, data breaches, and theft.

434. These actions also constitute deceptive and unfair acts or practices because Frontier knew the facts about its inadequate data security and failure to comply with applicable state and federal laws and industry standards would be unknown to and not easily discoverable by Plaintiff and Illinois Subclass members, and if known, would defeat Plaintiff's and Illinois Subclass

members' reasonable expectations regarding the security of their Private Information.

435. Frontier intended that Plaintiff and Illinois Subclass members rely on its deceptive and unfair acts and practices and the concealment and omission of material facts in connection with Frontier's offering of insurance products and services in Illinois.

436. Frontier's wrongful and deceptive acts and practices were and are injurious to the public because those practices were part of Frontier's generalized course of conduct that applied to the Illinois Subclass as a whole. Plaintiff and Illinois Subclass members have been adversely affected by Frontier's conduct and the public was and is at risk as a result thereof.

437. Frontier's wrongful and deceptive acts and practices in violation of the IFCA, as alleged herein, occurred primarily and substantially in Illinois.

438. As a direct and proximate result of Frontier's wrongful and deceptive conduct in violation of the IFCA, Plaintiff and Illinois Subclass members were injured in that they never would have provided their Private Information to Frontier or used Frontier's services had they known or been informed that Frontier failed to maintain and/or ensure sufficient security to keep Plaintiff and Illinois Subclass members' Private Information from being wrongfully accessed, taken, and misused by cybercriminals.

439. As a direct and proximate result of Frontier's violations of the ICFA, Plaintiff and Illinois Subclass members have suffered harm, including but not limited to (a) the lost or diminished value of their Private Information; (b) actual identity theft and fraud; (c) out-of-pocket and lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (d) loss of benefit of their bargain; (e) future costs in terms of time, effort, and money that will be expended for the remainder of their lives to prevent, detect, contest, and repair the impact of the Private Information compromised due to the

Data Breach; and (f) the continued and certainly increased risk to their Private Information, which remains unencrypted in Frontier's possession and subject to further unauthorized disclosures so long as Frontier fails to undertake appropriate and adequate measures to protect it.

440. Pursuant to 815 Ill. Comp. Stat. § 505/10a(a), Plaintiff and the Illinois Subclass seek actual and compensatory damages, injunctive relief, and court costs and attorneys' fees as a result of Frontier's violations of the ICFA.

COUNT IX: NEW YORK GENERAL BUSINESS LAW
N.Y. Gen. Bus. L. § 349 *et seq.* ("GBL")
(On Behalf of Plaintiff Burton and the New York Subclass)

441. Plaintiff Burton (for the purposes of this count, "Plaintiff") re-alleges and incorporates by reference paragraphs 1–146, 255–264, and 287–302 above as if fully set forth herein.

442. Frontier engaged in deceptive acts or practices in the conduct of its business, trade, and commerce or furnishing of services, in violation of the GBL, including without limitation through the following conduct:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and New York Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and New York Subclass members' Private Information, including duties imposed by the FTC Act, which was a direct and proximate cause of the Data

Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and New York Subclass members' Private Information, including by implementing and maintaining reasonable data security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and New York Subclass members' Private Information, including duties imposed by the FTC Act;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and New York Subclass members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and New York Subclass members' Private Information, including duties imposed by the FTC Act.

443. Frontier's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Frontier's data security measures and its ability to protect the confidentiality of consumers' Private Information.

444. Frontier acted intentionally, knowingly, and maliciously to violate New York's GBL, and recklessly disregarded Plaintiff's and New York Subclass members' rights.

445. As a direct and proximate result of Frontier's deceptive and unlawful acts and practices in violation of the GBL, Plaintiff and New York Subclass members have suffered and will continue to suffer injuries, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time

and expenses related to monitoring their financial and other accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Private Information; overpayment for Frontier's products and services; loss of the value of access to their Private Information; and the value of identity protection services made necessary by the Data Breach.

446. Frontier's deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large, including the residents of New York affected and harmed by the Data Breach.

447. Frontier's deceptive and unlawful practices and acts caused substantial injury to Plaintiff and New York Subclass members that they could not reasonably avoid.

448. Plaintiff and New York Subclass members seek all monetary and non-monetary relief allowed under the GBL, including actual damages or statutory damages of $50 (whichever is greater), treble damages, injunctive relief, and attorney's fees and costs.

COUNT X: UNITED STATES CABLE ACT
47 U.S.C. § 521 *et seq.*
(On behalf of Plaintiffs and the Nationwide Class, or alternatively, on behalf of the State Subclasses)

449. Plaintiffs re-allege and incorporate by reference paragraphs 1 through 302 above as if fully set forth herein

450. At all relevant times, Plaintiffs and Class Members were subscribers to Frontier's services.

451. At all relevant times, Frontier provided Plaintiffs and Class Members, as subscribers, one-way video and/or other programming services, and as such, provided a "cable service" as defined for purposes of 47 U.S.C. § 551. *See* 47 U.S.C. § 522(6).

452. At all relevant times, Frontier provided its one-way and/or other programming services to subscribers, including Plaintiffs and Class Members, through facilities consisting of a

set of closed transmission paths and associated signal generation, reception, and control equipment designed to provide cable services to multiple subscribers within a community, and as such, provided its services through a "cable system" as defined for purposes of 47 U.S.C. § 551. *See* 47 U.S.C. § 522(7).

453. At all relevant times, Frontier provided cable service to subscribers, including Plaintiffs and Class Members, over a cable system and, directly or through one or more affiliates, owned a significant interest in such cable system.

454. At all relevant times, Frontier provided cable service to subscribers, including Plaintiffs and Class Members, over a cable system and controlled or was responsible for, through any arrangement, the management and operation of such cable system.

455. At all relevant times, Frontier was a "cable operator" as defined for purposes of 47 U.S.C. § 551. *See* 47 U.S.C. § 522(5).

456. Pursuant to 47 U.S.C. § 551(b), Frontier, as a cable operator, is permitted to collect PII of its subscribers only in order to (i) obtain information necessary to render a cable service or other service provided by Frontier to the subscriber, or (ii) to detect unauthorized reception of cable communications.

457. Pursuant to 47 U.S.C. § 551(c)(1), Frontier, as a cable operator, is prohibited from disclosing PII concerning any subscriber without the subscriber's prior written consent.

458. Pursuant to 47 U.S.C. § 551(c)(1), Frontier, as a cable operator, is mandated to "take such actions as are necessary to prevent unauthorized access to [subscriber PII] by a person other than the subscriber or [Frontier]."

459. Pursuant to 47 U.S.C. § 551(e), Frontier, as a cable operator, is mandated to "destroy [PII] if the information is no longer necessary for the purpose for which it was collected" and there

are no pending requests for access to information by the subscriber or pursuant to court order.

460. Frontier disclosed and allowed unauthorized access to Plaintiffs' and Class Members' Private Information, including PII, in the Data Breach without prior notice to or consent of Plaintiffs and Class Members.

461. Frontier's disclosing and granting unauthorized access to Plaintiffs' and Class Members' Private Information, including PII, in the Data Breach without prior notice to or consent of Plaintiffs and Class Members violated 47 U.S.C. § 551(c)(1) and (c)(2)(C)(i).

462. Frontier failed to take necessary actions to prevent unauthorized disclosure to Plaintiffs' and Class Members' Private Information, including PII, in the Data Breach, including but not limited to by failing to implement and maintain industry standard and legally required data security policies and processes, which caused and allowed the Data Breach to happen.

463. Frontier's failure to take necessary actions to prevent unauthorized disclosure to Plaintiffs' and Class Members' Private Information, including PII, in the Data Breach violated 47 U.S.C. § 551(c)(1).

464. Frontier failed to destroy Plaintiffs' and Class Members' PII when it was no longer necessary for the purpose of rendering cable and/or other services to Plaintiffs and Class Members for which it was maintained to the extent it retained Plaintiffs' and Class Members' Private Information, including PII, in its network servers and systems after the subscriber-cable operator relationship had ended.

465. Frontier's failure to destroy Plaintiffs' and Class Members' Private Information, including PII, when it was no longer necessary for the purpose for which it was maintained violated 47 U.S.C. § 551(e).

466. As a direct and proximate result of Frontier's foregoing violations of 47 U.S.C. §

551, Plaintiffs' and Class Members' Private Information, including PII, was disclosed to and accessed by RansomHub from Frontier's network systems and servers, causing Plaintiffs and Class Members injuries and damages.

467. As current and former subscribers to Frontier's cable services, Plaintiffs and Class Members are persons aggrieved by Frontier's acts as a cable operator in violation of 47 U.S.C. § 551, including but not limited to Frontier's (a) disclosure and granting unauthorized access to Plaintiffs' and Class Members' Private Information, including PII, to the notorious ransomware group RansomHub in the Data Breach without prior notice to or consent of Plaintiffs and Class Members, (b) Frontier's failure to take necessary actions to prevent unauthorized disclosure to Plaintiffs' and Class Members' Private Information, including PII, in the Data Breach, and (c) failure to destroy Plaintiffs' and Class Members' Private Information, including PII, when it was no longer necessary for the purpose for which it was maintained.

468. As a direct and proximate result of Frontier's foregoing violations of 47 U.S.C. § 551, Plaintiffs and Class Members have suffered harm and attendant actual damages, including but not limited to (a) the lost or diminished value of their Private Information; (b) actual identity theft and fraud; (c) out-of-pocket and lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (d) loss of benefit of their bargain; (e) future costs in terms of time, effort, and money that will be expended for the remainder of their lives to prevent, detect, contest, and repair the impact of the Private Information compromised due to the Data Breach; and (f) the continued and certainly increased risk to their Private Information, which remains unencrypted in Frontier's possession and subject to further unauthorized disclosures so long as Frontier fails to undertake appropriate and adequate measures to protect it.

469. Pursuant to 47 U.S.C. § 551(f), Plaintiffs and Class Members, as persons aggrieved by Frontier's acts in violation of 47 U.S.C. § 551, are entitled to (a) actual damages not less than liquidated damages computed at the rate of $100 a day for each day of violation or $1,000, whichever is higher, (b) punitive damages, and (c) reasonable attorneys' fees and costs of litigation.

COUNT XI: UNJUST ENRICHMENT
(On behalf of Plaintiffs and the Nationwide Class, or alternatively, on behalf of the State Subclasses)

470. Plaintiffs re-allege and incorporate by reference paragraphs 1 through 302 above as if fully set forth herein.

471. This claim is pleaded in the alternative to the claims for breach of express contract and breach of implied contract.

472. Plaintiffs and Class Members conferred a direct benefit on Frontier by way of providing payment and their Private Information to Frontier as part of Frontier's business.

473. Frontier required Plaintiffs' and Class Members' Private Information to conduct its business and generate revenue, which it could not do without collecting and maintaining Plaintiffs' and Class Members' Private Information.

474. The monies Plaintiffs and Class Members paid to Frontier included a premium for Frontier's cybersecurity obligations and were supposed to be used by Frontier, in part, to pay for the administrative and other costs of providing reasonable data security and protection for Plaintiffs' and Class Members' Private Information.

475. Frontier enriched itself by hoarding the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Private Information. Instead of providing a reasonable level of security that would have prevented the hacking incident, Frontier calculated to increase its own profit at the expense of Plaintiffs and Class Members by utilizing

cheap, ineffective security measures and diverting those funds to its own personal use. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Frontier's decision to prioritize its own profits over the requisite security and the safety of their Private Information.

476. Frontier failed to provide reasonable security, safeguards, and protections to the Private Information of Plaintiffs and Class Members, and as a result, Frontier was overpaid.

477. Under principles of equity and good conscience, Frontier should not be permitted to retain the money Plaintiffs and Class Members paid it because Frontier failed to provide adequate safeguards and security measures to protect Plaintiffs' and Class Members' Private Information, which Plaintiffs and Class Members paid for but did not receive.

478. Frontier wrongfully accepted and retained these benefits—payment and Plaintiffs' and Class Members' Private Information—and was enriched to the detriment of Plaintiffs and Class Members.

479. Frontier's enrichment at Plaintiff's and Class Members' expense is unjust.

480. As a result of Frontier's wrongful conduct and resulting unjust enrichment, Plaintiffs and Class Members are entitled to restitution and disgorgement of profits, benefits, and other compensation obtained by Frontier, plus reasonable attorneys' fees and costs.

COUNT XII: DECLARATORY JUDGMENT
(On behalf of Plaintiffs and the Nationwide Class, or alternatively, on behalf of the State Subclasses)

481. Plaintiffs re-allege and incorporate by reference paragraphs 1 through 302 above as if fully set forth herein.

482. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant

further necessary supplemental relief. The Court has broad authority to restrain acts, such as those alleged herein, which are tortious and unlawful.

483. In the fallout of the Data Breach, a controversy has arisen about Frontier's duty to use reasonable data security for the Private Information it collects and maintains from customers.

484. On information and belief, Frontier's actions were—and *still* are—inadequate and unreasonable. Plaintiffs and Class Members continue to suffer injuries from the ongoing threat of fraud and identity theft due to Frontier's inadequate data security measures.

485. Given its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring as follows:

a. Frontier owed and continues to owe a legal duty to use reasonable data security to secure the Private Information entrusted to it;

b. Frontier breached, and continues to breach, its duties by failing to use reasonable measures to protect the Private Information entrusted to it from unauthorized access, use, and disclosure; and

c. Frontier's breaches of duties caused and continue to cause injuries to Plaintiffs and Class Members.

486. The Court should also issue injunctive relief requiring Frontier to use adequate security consistent with industry standards to protect the Private Information entrusted to it.

487. If an injunction is not issued, Plaintiffs and Class Members will suffer irreparable injuries and lack an adequate legal remedy if Frontier experiences a second data breach. And if a second breach occurs, Plaintiffs and Class Members will lack an adequate remedy at law because many of the resulting injuries are not readily quantified in full, and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages, while warranted for

out-of-pocket damages and other legally quantifiable and provable damages, cannot cover the full extent of Plaintiffs' and Class Members' injuries.

488. If an injunction is not issued, the resulting hardship to Plaintiffs and Class Members far exceeds the minimal hardship that Frontier could experience if an injunction is issued.

489. An injunction would benefit the public by preventing another data breach—thus preventing further injuries to Plaintiff, Class Members, and the public at large.

VIII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs Brian Carolus, Adrian Graham, Christopher Miller, Lauren Morgan, Marcelo Muto, Ian Terrell, Richard Retter, Joselyn Chiong, Timothy Morgan, James Pratt II, Seth Burton, Lori Rusk, and Gerald Wilson, individually and on behalf of all others similarly situated, pray for judgment as follows:

A. An Order certifying this case as a class action on behalf of Plaintiffs and the proposed Class, appointing Plaintiffs as class representative, and appointing their counsel to represent the Class;

B. Awarding Plaintiffs and the Class damages that include applicable compensatory, actual, statutory, nominal, exemplary, and punitive damages, as allowed by law;

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

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

E. Awarding injunctive relief in the form of additional technical and administrative cybersecurity controls as is necessary to protect the interests of Plaintiffs and the Class;

F. Enjoining Frontier from further deceptive practices and making untrue statements

about its data security, the Data Breach, and the transmitted Private Information;

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

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

I. Awarding such further relief to which Plaintiffs and the Class are entitled.

IX. DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all issues to triable.

Dated: September 9, 2024

Respectfully submitted,

/s/ Jeff Ostrow

Jeff Ostrow (admitted *pro hac vice*)
KOPELOWITZ OSTROW P.A.
One West Las Olas Blvd, Suite 500
Fort Lauderdale, FL 33301
Tel: (954) 525-4100
Fax: (954) 525-4300
ostrow@kolawyers.com

Gary Klinger (admitted *pro hac vice*)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Tel: 866-252-0878
Fax: 865-522-0049
gklinger@milberg.com

Tyler Bean (admitted *pro hac vice*)
SIRI & GLIMSTAD LLP
745 Fifth Ave., Suite 500
New York, NY 10151
Phone: (212) 532-1091
tbean@sirillp.com

Interim Co-Lead Counsel for Plaintiffs and the Putative Class

Joe Kendall
Texas Bar No. 11260700
KENDALL LAW GROUP, PLLC
3811 Turtle Creek Blvd., Suite 825

Dallas, Texas 75219
Tel: 214-744-3000
Fax: 214-744-3015
jkendall@kendalllawgroup.com

Interim Local Counsel for Plaintiffs and the Putative Class

CERTIFICATE OF SERVICE

I hereby certify that on September 9, 2024, the foregoing document was filed electronically with the Clerk of Court to be served by operations of the Court's electronic filing system on all parties of record.

s/ Jeff Ostrow
Jeff Ostrow