

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO**

GRACE STEAN , individually and on behalf of all others similarly situated, Plaintiff, vs. FRONTIER AIRLINES, INC. Defendant.	No. CIVIL ACTION CLASS ACTION COMPLAINT JURY TRIAL DEMANDED
---	---

Plaintiff Grace Stean (“Plaintiff”), individually and on behalf of all others similarly situated, brings this action against Defendant Frontier Airlines, Inc. (“Frontier”), to obtain damages, restitution, and injunctive relief from Defendant. Plaintiff makes the following allegations upon information and belief, except as to their own actions, the investigation of their counsel, and facts that are a matter of public record.

NATURE OF THE ACTION

1. This class action arises out of Defendant Frontier’s failures to properly secure, safeguard, encrypt, and/or timely and adequately destroy Plaintiff’s and Class members’ (defined below) sensitive personal identifiable information that it had acquired and stored for its business purposes.

2. According to its website, Defendant Frontier is a low fare airline that attempts to offer more than just low prices. “We are tireless in our efforts to save you money on your flights, but we know that low fares alone aren’t enough”¹

3. According to the data breach notice issued to Plaintiff on July 9, 2026, Frontier exposed the following personally identifiable information (“PII”), first and last name, address,

¹ <https://www.flyfrontier.com/about-us/> (last visited July 15, 2026)

phone number, Social Security Number, Driver's License Number, place of birth, designated contact information, passport number or visa number, date of birth and Frontier employee number.² On May 12, 2026 and on June 3, 2026, a known cybercriminal gang, Scattered Lapsus\$ Hunters was able to access and exfiltrate the PII of thousands of employees and potentially customers as well. (the "Data Breach")

4. Due to Defendant's data security failures which resulted in the Data Breach, cybercriminals were able to target Defendant's computer systems and exfiltrate Plaintiff's and Class members' highly sensitive Private Information. As a result of this Data Breach, Plaintiff's and Class Members' Private Information was compromised and stolen and remains in the hands of those cybercriminals.

5. Despite apparently learning of the Data Breach on or about June 18, 2026, and determining that Private Information was involved in the breach,³ Defendant failed to provide notice, or any information concerning the Breach to those affected, including Plaintiff and Class members until July 9, 2026. *See, e.g.*, Notice of Data Incident, attached as Exhibit "A."

6. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect Plaintiff's and Class members' Private Information with which it was entrusted for either treatment or employment or both.

7. Plaintiff brings this class action lawsuit on behalf of herself and all other similarly situated persons to address Defendant's inadequate safeguarding of Class members' Private Information that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class members that their information had been subject to the unauthorized

² See Notice of Data Incident attached as Exhibit A.

³ *Id.*

access of an unknown third party and failing to include in that belated and inadequate notice precisely what specific types of information were accessed and taken by cybercriminals.

8. Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant's computer network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the Data Breach and potential for improper disclosure of Plaintiff's and Class members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that network in a dangerous condition.

9. Defendant also failed to provide timely, accurate, and adequate notice to Plaintiff and other Class Members that their PII had been stolen, as well as precisely what types of information were stolen.

10. Defendant disregarded Plaintiff's and Class members' rights by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard Plaintiff's and Class members' Private Information; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiff and Class members with prompt and full notice of the Data Breach.

11. In addition, Defendant failed to properly monitor the computer network and systems that housed the Private Information. Had Defendant properly monitored its computer network and systems, it would have discovered the massive intrusion sooner rather than allowing cybercriminals unimpeded access to Plaintiff's and Class members' PII.

12. Plaintiff's and Class members' identities are now at risk because of Defendant's

negligent conduct since the Private Information that Defendant collected and maintained is now in the hands of data thieves.

13. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including: opening new financial accounts in Class members' names, taking out loans in Class members' names, using Class members' information to obtain government benefits, filing fraudulent tax returns using Class members' information, filing false medical claims using Class members' information, obtaining driver's licenses in Class members' names but with another person's photograph, and giving false information to police during an arrest.

14. As a result of the Data Breach, Plaintiff and Class members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class members must now and for years into the future closely monitor their financial accounts to guard against identity theft.

15. Plaintiff and Class members may also incur out of pocket costs for, *e.g.*, purchasing credit monitoring, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

16. Through this Complaint, Plaintiff seek to remedy these harms on behalf of herself and all other similarly situated individuals whose Private Information was accessed during the Data Breach.

17. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, as well as long-term and adequate credit monitoring funded by Defendant, and declaratory relief.

PARTIES

18. Plaintiff Grace Stean is and at all times mentioned herein was an individual citizen of the State of Colorado, and received a Notice of Data Incident, attached as Exhibit “A.”

19. Defendant Frontier Airlines, Inc. is a Colorado corporation with its principal place of business in Denver, Colorado. Defendant conducts business in Colorado and throughout the United States.

JURISDICTION AND VENUE

20. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act (“CAFA”), 28 U.S.C. §1332, because this is a class action wherein the amount in controversy exceeds the sum or value of \$5,000,000.00, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from each Defendant.

21. This Court has personal jurisdiction over the parties in this case. Defendant regularly conducts business and is headquartered in Colorado.

22. Venue is appropriate in this district because Defendant maintains a principal place of business and regularly conduct business here.

FACTUAL ALLEGATIONS Defendant’s Business

23. Defendant provides low fare airline services.

24. In the ordinary course of receiving Defendant’s services and products, each employee and customer must provide (and Plaintiff did provide) Defendant with sensitive, personal, and private information, such as their:

- Name, address, phone number, and email address;
- Date of birth;
- Social Security number;

- driver's license numbers;
- product information; and
- payment and financial account information.

25. Defendant agreed to and undertook legal duties to maintain the protected health and personal information entrusted to it by Plaintiff and Class members safely, confidentially, and in compliance with all applicable laws, including the Federal Trade Commission Act ("FTCA").

26. Yet, through its failure to properly secure Plaintiff's and Class members' Private Information, Defendant failed to meet its own promises of privacy.⁴

27. Thus, the potential for improper disclosure of Plaintiff's and Class members' PII was a known risk to Defendant and Defendant were on notice that failing to take steps necessary to secure the PII from those risks left its network in a dangerous condition.

28. Defendant failed to properly monitor the computer network and systems that housed the PII. Had Defendant properly monitored the network, it would have prevented this breach altogether.

The Data Breach

29. A data breach occurs when cyber criminals intend to access and steal Private Information that has not been adequately secured by a business entity like Defendant.

30. On or about July 9, 2026, Frontier announced that it experienced a security incident disrupting access to its systems. As above, the breach occurred when a known ransomware group, Scattered Lapsus\$ Hunters stole massive amounts of data from Defendant's information network.

31. Presently, however, Defendant has provided no public information on whether there was a ransom demand or payment.

⁴ <https://www.flyfrontier.com/legal/privacy-policy>

32. On information and belief, Plaintiff's and Class members' stolen Private Information has now been published by cybercriminals to the Dark Web as that is the modus operandi of ransomware attackers.⁵

33. As the Harvard Business Review notes, "[c]ybercriminals frequently use the Dark Web—a hub of criminal and illicit activity—to sell data from companies that they have gained unauthorized access to through credential stuffing attacks, phishing attacks, [or] hacking."⁶

34. The Data Breach occurred as a direct result of Defendant's failure to implement and follow basic security procedures to protect its employees' Private Information.

35. Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

36. Defendant had obligations created by FTCA, contract, industry standards, common law, and representations made to Plaintiff and Class members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

37. Plaintiff and Class members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

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

38. It is well known that PII, including Social Security numbers in particular, is a valuable commodity and a frequent, intentional target of cyber criminals. Companies that collect

⁵ <https://www.paloaltonetworks.com/cyberpedia/what-is-multi-extortion-ransomware> (Typically, in a ransomware attack, the criminal actor will not only encrypt the victim's system and block access until a ransom is paid but also exfiltrate data and threaten to release it to the dark web if a ransom is not paid. This scheme is known as a double-extortion attack. This scheme is used because many "organizations overcome the threat of file encryption with a simple up-to-date backup system.").

⁶ Brenda R. Sharton, *Your Company's Data Is for Sale on the Dark Web. Should You Buy It Back?*, HARVARD BUS. REV. (Jan. 4, 2023) <https://hbr.org/2023/01/your-companys-data-is-for-sale-on-the-dark-web-should-you-buy-it-back>.

such information, including Defendant, are well-aware of the risk of being targeted by cybercriminals.

39. Individuals place a high value on the privacy of their PII. Identity theft causes severe negative consequences to its victims, as well as severe distress and hours of lost time trying to fight against the impact of identity theft.

40. A data breach increases the risk of becoming a victim of identity theft. 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.”⁷

41. Individuals, like Plaintiff and Class members, are particularly concerned with protecting the privacy of their Social Security numbers, which are the key to stealing any person’s identity and is likened to accessing one’s DNA for hacker’s purposes.

42. Data Breach victims suffer long-term consequences when their Social Security numbers are taken and used by hackers. Even if they know their Social Security numbers are being misused, Plaintiff and Class members cannot obtain new numbers unless they become a victim of Social Security number misuse.

⁷ “Victims of Identity Theft, 2018,” U.S. Department of Justice (April 2021, NCJ 256085) available at: <https://bjs.ojp.gov/content/pub/pdf/vit18.pdf> (last visited July 15, 2026).

43. The Social Security Administration has warned that “a new number probably won’t solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So, using a new number won’t guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.”⁸

44. Unfortunately, these preventable cases will largely come from “misconfigurations, human error, poor maintenance, and unknown assets.”⁹

45. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, and hopefully can ward off a cyberattack.

46. According to an FBI publication, “[r]ansomware is a type of malicious software, or malware, that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return. Ransomware attacks can cause costly disruptions to operations and the loss of critical information and data.”¹⁰ This publication also explains that “[t]he FBI does not support paying a ransom in response to a ransomware attack. Paying a ransom doesn’t guarantee you or your organization will get any data back. It also encourages perpetrators to target more victims and offers an incentive for others to get involved in this type of illegal activity.”¹¹

⁸ <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last visited July 15, 2026).

⁹ <https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/?sh=176bb6887864> (last visited July 15, 2026).

¹⁰ <https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/ransomware> (last visited July 15, 2026).

¹¹ *Id.*

47. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgments of data security compromises, and despite its own acknowledgment of its duties to keep PII private and secure, Defendant failed to take appropriate steps to protect Plaintiff's and the proposed Class' PII from being compromised.

Defendant Failed to Comply with FTC Guidelines.

48. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which 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.

49. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal patient information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.¹² The 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.¹³

50. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords

¹² *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited July 15, 2026).

¹³ *Id.*

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.

51. The FTC has brought enforcement actions against businesses, like that of Defendant, for failing to adequately and reasonably protect employee and customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

52. These FTC enforcement actions include actions against airlines like Defendant.

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

54. Defendant was at all times fully aware of its obligation to protect the PII of its employees and customers. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Failed to Comply with Industry Standards.

55. As shown above, experts studying cyber security routinely identify service providers as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

56. Several best practices have been identified that a minimum should be implemented by companies like Defendant, including but not limited to: educating all employees; utilizing strong passwords; creating multi-layer security, including firewalls, anti-virus, and anti-malware

software; encryption, making data unreadable without a key; using multi-factor authentication; protecting backup data, and; limiting which employees can access sensitive data.

57. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

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

59. These frameworks are existing and applicable industry standards in the healthcare industry, yet Defendant failed to comply with these accepted standards, thereby opening the door to and failing to thwart the Data Breach.

Data Breaches Put Consumers at an Increased Risk Of Fraud and Identity Theft

60. Data Breaches such as the one Plaintiff and Class members experienced cause significant disruption to the overall daily lives of victims affected by the attack.

61. In 2019, the United States Government Accountability Office released a report addressing the steps consumers can take after a data breach.¹⁴ Its appendix of steps consumers should consider, in extremely simplified terms, continues for five pages. In addition to explaining

¹⁴ <https://www.gao.gov/assets/gao-19-230.pdf> (last visited July 15, 2026).

specific options and how they can help, one column of the chart explains the limitations of the consumers' options. It is clear from the GAO's recommendations that the steps Data Breach victims (like Plaintiff and Class) must take after a breach like Defendant's are both time consuming and of only limited and short-term effectiveness.

62. The GAO has long recognized that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."

63. The FTC, like the GAO, recommends that identity theft 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 7 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.¹⁵

64. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

65. 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.

66. Theft of Private Information is also gravely serious. PII is valuable property.¹⁶

67. It must also be noted there may be a substantial time lag – measured in years --

¹⁵ See *GOA Report* at 19.

¹⁶ See, e.g., John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

between when harm occurs versus when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used. According to GAO:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See 2007 GAO Report, at p. 29.

68. Private Information and financial information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the “cyber black-market” for years.

69. There is a strong probability that the entirety of the stolen information has been dumped on the black market or will be dumped on the black market, meaning Plaintiff and Class members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiff and Class members must vigilantly monitor their financial and medical accounts for many years to come.

70. Furthermore, the Social Security Administration has warned that identity thieves can use an individual’s Social Security number to apply for additional credit lines.¹⁷ Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.¹⁸ Each of these fraudulent activities is difficult to detect. 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

¹⁷ *Identity Theft and Your Social Security Number*, Social Security Administration (2018) at 1. Available at <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last visited July 15, 2026).

¹⁸ *Id.* at 4.

employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

71. Moreover, it is not an 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. Even then, a 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.”¹⁹

72. This data, as one would expect, commands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, “[c]ompared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market.”²⁰

Plaintiff Grace Steans' Experiences

73. Plaintiff Grace Stean is a Data Breach victim, having received her Notice of Data Incident on or after July 9, 2026. See Exhibit A.

74. Since the Data Breach, Plaintiff Stean has tried to mitigate the damage by changing her passwords, contacting the credit bureaus as Defendant instructed, and monitoring her financial accounts for about 2 and a half hours per week. This is more time than she spent prior to learning of the Defendant's Data Breach. Having to do this every week not only wastes her time as a result of Defendant's negligence, but it also causes her great anxiety.

¹⁹ 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 July 15, 2026).

²⁰ Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), <http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last visited July 15, 2026).

75. Soon after the Data Breach, Plaintiff Stean began receiving an excessive number of spam calls on the same cell phone number provided to Defendant on her records. These calls are a distraction, must be deleted, and waste time each day. Given the timing of the Data Breach, she believes that the calls are related to her stolen PII.

76. Plaintiff Stean is aware that cybercriminals often sell Private Information, and once stolen, it is likely to be abused months or even years after Defendant's Data Breach.

77. Plaintiff has suffered imminent and impending injury arising from the present and ongoing risk of fraud, identity theft, and misuse resulting from her PII being placed in the hands of unauthorized third parties and possibly criminals. Plaintiff suffered lost time, annoyance, interference, and inconvenience because of the Data Breach.

78. Plaintiff has experienced anxiety and increased concerns arising from the fact that her PII has been or will be misused and from the loss of her privacy.

79. The risk is not hypothetical. Here, a known hacking group intentionally stole the data, misused it, threatened to publish, or has published it on the Dark Web, and the sensitive information, including names and Social Security numbers, is the type that could be used to perpetrate identity theft or fraud.

80. Plaintiff further suffered actual injury in the form of damages to and diminution in the value of Plaintiff's PII—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and because of the Data Breach. Future identity theft monitoring is reasonable and necessary, and such will include future costs and expenses.

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

82. Had Plaintiff Stean been aware that Defendant's computer systems were not secure, she would not have entrusted Defendant with her PII.

Plaintiff's And Class Members' Common Injuries

83. To date, Defendant has done absolutely nothing to compensate Plaintiff and Class members for the damages they sustained in the Data Breach.

84. Furthermore, Defendant's failure to safeguard Plaintiff's and Class members' Private Information, places the burden squarely on Plaintiff and the Class, rather than on the Defendant, to investigate and protect themselves from Defendant's tortious acts and omissions resulting in the Data Breach.

85. Plaintiff and Class members have been damaged by the compromise and exfiltration, by cyber-criminals, of their Private Information as a result of the Data Breach, and by the severe disruption to their lives as a direct and foreseeable consequence of this Data Breach.

86. Plaintiff and Class members were damaged in that their Private Information is now in the hands of cyber criminals being sold and potentially for sale for years into the future.

87. As a direct and proximate result of Defendant's conduct, Plaintiff and Class members have been placed at an actual, imminent, and substantial risk of harm from fraud and identity theft, especially in light of the actual fraudulent misuse of the Private Information that has already taken place, as alleged herein.

88. As a direct and proximate result of Defendant's conduct, Plaintiff and Class members have been forced to expend time dealing with the effects of the Data Breach.

89. Plaintiff and Class members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, for medical care and services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft. Plaintiff and Class

members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

90. Plaintiff and Class members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiff and Class members.

91. Plaintiff and Class members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

92. Plaintiff and Class members have spent and will continue to spend significant amounts of time to monitor their financial accounts and records for misuse.

93. Plaintiff and Class members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

- a. Finding fraudulent charges;
- b. Canceling and reissuing credit and debit cards;
- c. Purchasing credit monitoring and identity theft prevention;
- d. Monitoring their medical records for fraudulent charges and data;
- e. Addressing their inability to withdraw funds linked to compromised accounts;
- f. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

- g. Placing “freezes” and “alerts” with credit reporting agencies;
- h. Spending time on the phone with or at a financial institution to dispute fraudulent charges;
- i. Contacting financial institutions and closing or modifying financial accounts;
- j. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;
- k. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and
- l. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

Moreover, Plaintiff and Class members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing personal and financial information is not accessible online and that access to such data is password-protected.

94. Further, as a result of Defendant’s conduct, Plaintiff and Class members are forced to live with the anxiety that their Private Information—which contains the most intimate details about a person’s life—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

95. Defendant’s delay in identifying and reporting the Data Breach caused additional harm. In a data breach, time is of the essence to reduce the imminent misuse of PII. Early notification helps a victim of a Data Breach mitigate their injuries, and in the converse, delayed

notification causes more harm and increases the risk of identity theft. Here, Defendant knew of the breach June 18, 2026 and has only notified those affected, including Plaintiff and Class members on July 9, 2026.

CLASS ALLEGATIONS

96. Plaintiff brings this nationwide class action individually and on behalf of all other persons similarly situated (the “Class”) pursuant to Federal Rule of Civil Procedure 23(a) and (b)(3).

97. Plaintiff proposes the following Class definition, subject to amendment based on information obtained through discovery:

Nationwide Class:

All individuals whose Private Information was compromised in the Data Breach beginning in May 2026 and who were sent a Notice Letter (“the “Class”).

98. Excluded from the Class are Defendant’s officers, directors, and employees; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

99. Plaintiff reserves the right to amend the definition of the Class or add a class or subclass if further information and discovery indicate that the definition of the Class should be narrowed, expanded, or otherwise modified.

100. Certification of Plaintiff’s claim for class-wide treatment is appropriate because Plaintiff can prove the elements of Class Members’ claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims for each Class Member.

101. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under Rule 23 of the Federal Rules of Civil Procedure:

102. **Numerosity:** The members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Private Information of thousands of employees and customers of Defendant were compromised in the Data Breach. Such information is readily ascertainable from Defendant's records.

103. **Commonality:** There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

- a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;
- b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations including, *e.g.*, the FTC Act;
- d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;
- e. Whether hackers obtained Plaintiff's and Class Members' Private Information in the Data Breach;
- f. Whether Defendant knew or should have known that its data security systems and

monitoring processes were deficient;

- g. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;
- h. Whether Defendant breached the covenant of good faith and fair dealing implied in its contracts with Plaintiff and Class Members; and
- i. Whether Plaintiff and the Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

104. **Typicality:** The claims or defenses of Plaintiff are typical of the claims or defenses of the proposed Class because Plaintiff's claims are based upon the same legal theories and same violations of law. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class Member, was compromised in the Data Breach.

105. This lawsuit presents no difficulties that would impede its management by the Court as a class action. The class certification issues can be easily determined because the Class includes only Defendant's employees, the legal and factual issues are narrow and easily defined, and the Class Membership is limited. The Class does not contain so many persons that would make the Class notice procedures unworkable or overly expensive. The identity of the Class Members can be identified from Defendant's records, such that direct notice to the Class Members would be appropriate.

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

107. Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of

this matter and the parties' interests therein. Such particular issues include, but are not limited to:

- a. Whether Defendant failed to timely and adequately notify the public of the Data Breach;
- b. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;
- c. Whether Defendant's security measures to protect its data systems were reasonable in light of best practices recommended by data security experts;
- d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;
- e. Whether Defendant failed to take commercially reasonable steps to safeguard employees' Private Information; and
- f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

108. Further, this action satisfies Rule 23 because: (i) common questions of law and fact predominate over any individualized questions; (ii) prosecuting individual actions would create a risk of inconsistent or varying adjudications, risking incompatible standards of conduct for Defendant, and a risk adjudications with respect to individual members of the Class which would as a practical matter be dispositive of the interests of the other members not parties to the adjudications or would substantially impair or impede their ability to protect their interest; and (iii) the Defendant have acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive relief or corresponding declaratory relief with respect to the Class as a whole.

109. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

CAUSES OF ACTION
COUNT I
Negligence
(On Behalf of Plaintiff and Class Members)

110. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

111. Defendant required Plaintiff and Class members to submit non-public personal information in order to airline services and/or employment.

112. By collecting and storing this data in Defendant's computer network and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard its computer network—and Class members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a Data Breach.

113. Defendant owed a duty of care to Plaintiff and Class members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

114. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its employees, which is recognized by laws and regulations as well as common law. Defendant was in a position to ensure that its systems were

sufficient to protect against the foreseeable risk of harm to Class members from a Data Breach.

115. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits “unfair . . . 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.

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

117. Defendant breached its duties, and thus were negligent, by failing to use reasonable measures to protect Class members’ Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

- a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class members’ Private Information;
- b. Failing to adequately monitor the security of its networks and systems;
- c. Failure to periodically ensure that its email system had plans in place to maintain reasonable data security safeguards;
- d. Allowing unauthorized access to Class members’ Private Information;
- e. Failing to detect in a timely manner that Class members’ Private Information had been compromised; and
- f. Failing to timely notify Class members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

118. It was foreseeable that Defendant’s failure to use reasonable measures to protect

Class members' Private Information would result in injury to Class members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

119. It was therefore foreseeable that the failure to adequately safeguard Class members' Private Information would result in one or more types of injuries to Class members.

120. Plaintiff and Class members are entitled to compensatory and consequential damages suffered because of the Data Breach.

121. Defendant's negligent conduct is ongoing, in that it still holds the Private Information of Plaintiff and Class members in an unsafe and unsecure manner.

122. Plaintiff and Class members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class members.

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

123. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

124. Pursuant to the Federal Trade Commission Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class members' Private Information.

125. Defendant breached its duties to Plaintiff and Class members under the Federal Trade Commission Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class members' Private Information.

126. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se*.

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

128. The injury and harm suffered by Plaintiff and Class members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it failed to meet its duties, and that Defendant's breach would cause Plaintiff and Class members to experience the foreseeable harms associated with the exposure of their Private Information.

129. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

COUNT III
Breach Of Third Party Beneficiary Contract
(On Behalf of Plaintiff and Class Members)

130. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

131. As discussed above, Defendant entered into contracts, written or implied, with its clients to perform services. Upon information and belief, these contracts are virtually identical between and among Defendant and its clients around the country on behalf of which Defendant provided services for consumers, including Plaintiff and Class Members affected by the Data Breach.

132. In exchange, Defendant agreed, in part, to implement adequate security measures to safeguard the Private Information of Plaintiff and the Class.

133. These contracts were made expressly for the benefit of Plaintiff and the Class, as

Plaintiff and Class Members were the intended third-party beneficiaries of the contracts.

134. Defendant knew that if it were to breach these contracts, consumers for which it was providing services, Plaintiff and Class Members, would be harmed.

135. Defendant breached the contracts by, among *inter alia*, failing to (i) use reasonable data security measures, (ii) implement adequate protocols and employee training sufficient to protect Plaintiff Private Information from unauthorized disclosure to third parties, and (iii) promptly and adequately detecting the Data Breach and notifying Plaintiff and Class Members thereof.

136. Plaintiff and the Class were harmed by Defendant's breach of its contracts with its clients, as such breach is alleged herein, and are entitled to the losses and damages they have sustained as a direct and proximate result thereof.

137. Plaintiff and Class Members are also entitled to their costs and attorney's fees incurred in this action.

138. As a direct and proximate result of Defendant's conduct, Plaintiff and Class members suffered and will continue to suffer damages in an amount to be proven at trial.

139. In addition to monetary relief, Plaintiff and Class members are also entitled to injunctive relief requiring Defendant to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide credit monitoring and identity theft insurance to Plaintiff and Class members for a period of ten years.

COUNT IV
Breach of Implied Contract
(On Behalf of Plaintiff and Class Members)

140. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

141. This Claim is pleaded in the alternative to Count III above.

142. When Plaintiff and Class members provided their Private Information to Defendant in exchange for Defendant's services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

143. Defendant solicited, offered, and invited Class members to provide their Private Information as part of Defendant's regular business practices. Plaintiff and Class members accepted Defendant's offers and provided their Private Information to Defendant.

144. In entering into such implied contracts, Plaintiff and Class members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations, and were consistent with industry standards.

145. Plaintiff and Class members paid money to Defendant with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so.

146. Plaintiff and Class members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

147. Plaintiff and Class members would not have entrusted their Private Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

148. Plaintiff and Class members fully and adequately performed their obligations under the implied contracts with Defendant.

149. Defendant breached its implied contracts with Class members by failing to safeguard and protect their Private Information.

150. As a direct and proximate result of Defendant's breach of the implied contracts, Class members sustained damages as alleged herein, including the loss of the benefit of the bargain.

151. Plaintiff and Class members are entitled to compensatory, consequential, and nominal damages suffered because of the Data Breach.

152. Plaintiff and Class members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate long-term credit monitoring to all Class members.

COUNT V
Unjust Enrichment
(On Behalf of Plaintiff and Class Members)

153. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

154. Plaintiff brings this claim individually and on behalf of all Class members.

155. This Claim is pleaded in the alternative to Counts III and IV above.

156. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments made by or on behalf of Plaintiff and the Class members.

157. As such, a portion of the payments made by or on behalf of Plaintiff and the Class members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

158. Plaintiff and Class members conferred a monetary benefit on Defendant. Specifically, they purchased services from Defendant and/or its agents or were employed by

Defendant and in so doing provided Defendant with their Private Information. In exchange, Plaintiff and Class members should have received from Defendant the services that were the subject of the transaction and have their Private Information protected with adequate data security.

159. Defendant knew that Plaintiff and Class members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the Private Information of Plaintiff and Class members for business purposes.

160. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class members' Private Information. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to increase its own profits at the expense of Plaintiff and Class members by utilizing cheaper, ineffective security measures. Plaintiff and Class members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security.

161. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

162. Defendant failed to secure Plaintiff's and Class members' Private Information and, therefore, did not provide full compensation for the benefit Plaintiff and Class members provided.

163. Defendant acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

164. If Plaintiff and Class members knew that Defendant had not reasonably secured their Private Information, they would not have agreed to provide their Private Information to

Defendant.

165. Plaintiff and Class members have no adequate remedy at law.

166. As a direct and proximate result of Defendant's conduct, Plaintiff and Class members have suffered and will suffer injury, including but not limited to: (a) actual identity theft; (b) the loss of the opportunity of how their Private Information is used; (c) the compromise, publication, and/or theft of their Private Information; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (e) lost opportunity costs associated with efforts expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (f) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Private Information in its continued possession; and (g) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class members.

167. As a direct and proximate result of Defendant's conduct, Plaintiff and Class members have suffered and will continue to suffer other forms of injury and/or harm.

168. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class members overpaid for Defendant's services.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and all similarly situated others, pray for relief as follows:

- a. For an Order certifying this action as a Class action and appointing Plaintiff as a Class Representative and their counsel as Class Counsel;
- b. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class members' PII, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class members;
- c. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to employee and consumer data collection, storage, and safety, and to disclose with specificity the type of Personal Information compromised during the Data Breach;
- d. Ordering Defendant to pay for not less than three years of credit monitoring for Plaintiff and the Class;
- e. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;
- f. For an award of punitive damages, as allowable by law;
- g. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;
- h. Pre-and post-judgment interest on any amounts awarded; and,
- i. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury on all claims so triable.

Dated: July 15, 2026

Respectfully submitted,

By: /s/ Liberato P. Verderame

Liberato P. Verderame

(ID No. 2687549)

Marc H. Edelson (ID No. 2688361)

EDELSON LECHTZIN LLP

411 S. State Street, Suite N300

Newtown, PA 18940

T: (215) 867-2399

medelson@edelson-law.com

lverderame@edelson-law.com

Attorneys for Plaintiff and the Putative Class