FRONTIER
Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

July 9, 2026

Q1417-L01-0000001 P001 T00001 ********SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L01 EMPLOYEES (ALL STATES EXCEPT MA)
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789

RE: Notice of Data Breach

Dear Sample A. Sample:

Frontier Airlines ("Frontier") recently discovered a data security incident that may affect certain data related to you. We want to provide you with information about the incident, steps we are taking in response, and steps you may elect to take to guard against identity theft and fraud.

What Happened? On June 18, 2026, Frontier determined that an unauthorized third party had accessed a Frontier data storage account containing files with certain personal information. In connection with the incident, Frontier immediately initiated our incident response protocols, notified law enforcement, and engaged a third-party cybersecurity firm to conduct a comprehensive investigation. This investigation found that certain information may have been accessed or downloaded without authorization from the data storage account on May 12, 2026, and on June 3, 2026. At this time, Frontier believes that this incident has been contained and has no evidence of continued unauthorized access to Frontier systems in connection with this incident.

What Information Was Involved? We determined that the information involved in this incident may include some or all of the following information about you: first and last name, address, 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 ID number.

What We Are Doing. The security of our systems is a top priority for Frontier, and we take this matter very seriously. In response to this incident, we immediately took steps to secure the account and help prevent a reoccurrence of this type of incident, including strengthening access controls, improving monitoring of our systems, and implementing other measures to safeguard information and enhance our ability to detect and respond to potential threats. Additionally, we are offering complimentary credit monitoring and other identity protection services through Experian IdentityWorks^{SM} to all Frontier team members potentially affected by this incident. Please refer to Attachment A for more details.

What You Can Do. It is always advisable to remain vigilant against attempts at fraud or identity theft, which includes carefully reviewing online and financial accounts and credit reports for suspicious activity. This is a best practice for all individuals. If you enroll in Experian IdentityWorks^{SM}, you also will have access to fraud detection tools. Additionally, in Attachment B, we have enclosed instructions for how you can contact the three major credit reporting agencies and other tips you may want to consider to protect your personal information.

For More Information. We sincerely regret any inconvenience or concern caused by this incident. If you have further questions or concerns, please call our dedicated assistance line at 833-931-4244 (toll-free), Monday through Friday, from 9:00 a.m. to 9:00 p.m. Eastern time (excluding U.S. holidays).

Sincerely,

Steve Schuller
Senior Vice President, Human Resources

0000001

Attachment A

To help protect your identity, we are offering complimentary access to Experian IdentityWorks℠ for 12 months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for 12 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 12-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** October 31, 2026 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/1Bcredit
- Provide your **activation code**: ABCDEFGHI

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 833-931-4244 by October 31, 2026. Be prepared to provide engagement number ENGAGE# as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Attachment B

Below are additional helpful tips you may want to consider to protect your personal information.

Review Your Credit Reports and Account Statements; Notify Law Enforcement of Suspicious Activity
As a precautionary measure, we recommend that you remain vigilant by reviewing your credit reports and account statements closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or other company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact law enforcement, the Federal Trade Commission ("FTC"), and/or the Attorney General's office in your home state. You can also contact these agencies for information on how to prevent or avoid identity theft, and you can contact the FTC at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
http://www.identitytheft.gov/
1-877-IDTHEFT (438-4338)

Copy of Credit Report
You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting https://www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to the Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can print this form at https://www.annualcreditreport.com/manualRequestForm.action. Credit reporting agency contact details are provided below.

Experian:	Equifax:	TransUnion:
experian.com	equifax.com	transunion.com
experian.com/help	equifax.com/personal/credit-report-services	transunion.com/credit-help
P.O. Box 2002	P.O. Box 740241	P.O. Box 1000
Allen, TX 75013	Atlanta, GA 30374	Chester, PA 19016
888-397-3742	800-685-1111	888-909-8872

When you receive your credit reports, review them carefully. Look for accounts or credit inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is inaccurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

Fraud Alert
You may want to consider placing a fraud alert on your credit file. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. If you have already been a victim of identity theft, you may have an extended alert placed on your report if you provide the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above.

Security Freeze
You have the right to place a security freeze on your credit file free of charge. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. As a result, using a security freeze may delay your ability to obtain credit. In order to place a security freeze, you may be required to provide the credit reporting agency with information that identifies you including your full name; social security number; date of birth; current and previous addresses; a copy of your state-issued identification card; and a recent utility bill, bank statement, or telephone bill.

Credit reporting agencies have three business days after receiving your request to place a security freeze, or one business day for requests made electronically or by toll-free telephone. They must also send written confirmation to you within five business days and provide you with a unique personal identification number (PIN) and/or password that can be used to authorize the removal or lifting of the security freeze.

0000001

Credit reporting agencies must lift a security freeze within three business days after receiving your request by mail, or one hour after receiving your request electronically or by toll-free telephone. To remove or temporarily lift the security freeze to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail or electronically, and include: proper identification (name, address, and Social Security number); the PIN or password provided to you when you placed the security freeze; and the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available.

Federal Fair Credit Reporting Act Rights
The Fair Credit Reporting Act ("FCRA") is federal legislation that regulates how credit reporting agencies use your information. It promotes the accuracy, fairness, and privacy of consumer information in the files of credit reporting agencies. As a consumer, you have certain rights under the FCRA, which the FTC has summarized as follows: you must be told if information in your file has been used against you; you have the right to know what is in your file; you have the right to ask for a credit score; you have the right to dispute incomplete or inaccurate information; credit reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; credit reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. Identity theft victims and active-duty military personnel have additional rights.

For more information about these rights, you may go to www.ftc.gov/credit or write to: Consumer Response Center, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580.

Additional Information
If you are the victim of fraud or identity theft, you also have the right to file a police report.

You may consider starting a file with copies of your credit reports, any police report, any correspondence, and copies of disputed bills. It is also useful to keep a log of your conversations with creditors, law enforcement officials, and other relevant parties.

For California and Wyoming residents: Notification was not delayed due to a law enforcement investigation.

For Colorado and Illinois residents: You may obtain information from the Federal Trade Commission and the credit reporting agencies about fraud alerts and security freezes.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and the state Attorney General.

For Maryland residents: You may contact the Office of the Maryland Attorney General, 200 St. Paul Place, Baltimore, MD 21202, http://www.oag.maryland.gov, 1-888-743-0023. The Office of the Maryland Attorney General may be able to provide you with information about the steps you can take to avoid identity theft.

For New York residents: For more information on identity theft, you can contact the following: New York Department of State Division of Consumer Protection at http://www.dos.ny.gov/consumer-protection or (800) 697-1220 or New York State Attorney General at https://ag.ny.gov/ or (800) 771-7755.

For New Mexico residents: You have rights pursuant to the FCRA, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the FCRA, the credit reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; credit reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the FCRA not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the FCRA. For more information about these rights, you may go to www.ftc.gov/credit or write to: Consumer Response Center, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27699-9001, http://www.ncdoj.gov, 1-877-566-7226. You are also advised to report any suspected identity theft to law enforcement or to the North Carolina Attorney General. The North Carolina Attorney General may be able to provide you with information about preventing identity theft.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and the Oregon Attorney General. For more information on security freezes, you can visit the Oregon Department of Financial Regulation website at https://dfr.oregon.gov/financial/protect/Pages/place-credit-freeze.aspx.

For Rhode Island residents: The Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this event. There are approximately seven Rhode Island residents impacted by this event.

For Washington, D.C. residents: You may contact the Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington, D.C. 20001, http://oag.dc.gov, 1-202-727-3400. The Office of the Attorney General for the District of Columbia may be able to provide you with information about the steps you can take to avoid identity theft.

For Arizona, California, Iowa, New York, North Carolina, Oregon, Washington, and Washington, D.C., and West Virginia residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit bureaus directly to obtain such additional report(s).