

October 24, 2024

NORTON ROSE FULBRIGHT

Norton Rose Fulbright US LLP
1550 Lamar Street, Suite 2000
Houston, Texas 77010-4106
United States of America

Direct line +1 713 651 5684
will.daugherty@nortonrosefulbright.com

Tel +1 713 651 5151
Fax +1 713 651 5246

Via Certified Mail

Office of the Attorney General
Attn: Data Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Legal Notice of Data Incident

Dear Sir or Madam:

I am writing on behalf of my client, Southwest Airlines Co. ("Southwest"), to notify you of a cybersecurity incident.

Southwest recently discovered that an unauthorized third party gained access to certain employees' Workday accounts. Southwest immediately began an investigation to determine the nature and scope of the incident. The investigation determined that certain employees' credentials were compromised, and as a result, an unauthorized actor accessed and changed certain employees' direct deposit information between August 16, 2024 and September 19, 2024. Upon learning this, Southwest took action to secure employees' Workday accounts. The investigation also identified a fake Southwest website designed to trick employees into providing their Workday credentials on the fake site.

On October 7, 2024, Southwest completed its review of the data and identified personal information belonging to certain of Southwest's employees including name, address, bank account number, and pay slips belonging to four (4) Maryland residents.

Today, October 24, 2024, Southwest will begin mailing notification letters to the four (4) Maryland residents. A sample copy of the notification letter is attached. Southwest will also be offering 12 months of complimentary credit monitoring and fraud protection services to these individuals. Southwest is also providing a telephone number for individuals to call with any questions regarding the incident.

To help prevent this type of incident from occurring, Southwest has provided additional security awareness education to employees and implemented additional security measures around employee access to Workday, including implementing step-up MFA for accessing banking information, and expediting the completion of deployment of multi-factor authentication for employees' remote access to Workday.

If you have any questions or need further information regarding this Incident, please do not hesitate to contact me.

Sincerely,



Will Daugherty



Norton Rose Fulbright US LLP is a limited liability partnership registered under the laws of Texas.

Norton Rose Fulbright US LLP, Norton Rose Fulbright LLP, Norton Rose Fulbright Australia, Norton Rose Fulbright Canada LLP and Norton Rose Fulbright South Africa Inc are separate legal entities and all of them are members of Norton Rose Fulbright Verein, a Swiss verein. Norton Rose Fulbright Verein helps coordinate the activities of the members but does not itself provide legal services to clients. Details of each entity, with certain regulatory information, are available at nortonrosefulbright.com.



Return Mail Processing
PO Box 999
Suwanee, GA 30024

11160*****SNGLP

SAMPLE A. SAMPLE - L01

APT ABC

123 ANY ST

ANYTOWN, US 12345-6789



October 24, 2024

RE: NOTICE OF DATA INCIDENT

Dear Sample A. Sample,

Southwest recognizes the importance of the privacy and confidentiality of employees' personal information. We are writing to provide you with additional information on an incident involving your personal information within your Workday account that we previously communicated with you about. This notice describes the Incident, outlines the measures we have taken in response, and provides information on additional steps you may consider taking to protect your information.

What Happened?

We recently discovered suspicious activity within certain employees' Workday accounts. We immediately launched an investigation to determine the nature and scope of the incident. Through this investigation, we determined that your credentials were compromised, and as a result, an unauthorized person changed your direct deposit information in your Workday account during the period from August 16, 2024 to September 19, 2024. Upon learning this, we took action to secure your Workday account. During our investigation, we also identified a fake Southwest website designed to trick employees into providing their Workday credentials on the fake site.

What Information Was Involved?

The personal information that may have been accessed in your Workday account includes your name, address, bank account number, and pay slips.

What We Are Doing?

To help prevent this type of incident from happening again, we have enhanced security around employee access to Workday and provided additional security awareness training to employees.

As a precaution, we are offering you a complimentary 12-month membership in Experian® IdentityWorksSM Credit 1B. This product helps detect possible misuse of your personal information and provides you with identity protection support focused on immediate identification and resolution of identity theft. IdentityWorks is completely free to you and enrolling in this program will not hurt your credit score.

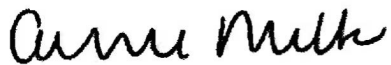
What You Can Do?

We encourage you to review the additional information on IdentityWorks, including instructions on how to activate your complimentary 12-month membership, as well as information on additional steps you can take in response to this incident, on the pages that follow this letter.

For More Information.

If you have questions, please call (877) 792-4792 Monday through Friday between the hours of 9:00 a.m. and 6:00 p.m. Central Time.

Sincerely,

A handwritten signature in black ink, appearing to read "Carrie Mills". The script is cursive and fluid.

Carrie Mills

Vice President and Chief Information Security Officer

Experian Enrollment Information

To help protect your identity, we are offering a complimentary one-year membership of Experian's® IdentityWorksSM. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you enroll by: **January 31, 2025** (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your activation code: ABCDEFGHI

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at (833) 931-7577 by **January 31, 2025**. Be prepared to provide engagement number **B133803** 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 files 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.
- **Up to \$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at (833) 931-7577. 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 (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 this Identity Restoration support is available to you for two years 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. You will also find self-help tips and information about identity protection at this site.

* 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.

Information About Additional Steps You Can Take

Contact information for the three nationwide credit reporting companies is as follows:

Equifax	Experian	TransUnion
Phone: 1-800-685-1111 P.O. Box 740256 Atlanta, Georgia 30348 www.equifax.com	Phone: 1-888-397-3742 P.O. Box 9554 Allen, Texas 75013 www.experian.com	Phone: 1-888-909-8872 P.O. Box 2000 Chester PA 19016 www.transunion.com

Free Credit Report. We remind you to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. If you identify any unauthorized charges on your financial account statements, you should immediately report any such charges to your financial institution. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, and Maryland 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 reporting agencies directly to obtain such additional report(s).

Security Freeze. Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator or have a valid power of attorney, you can get a free freeze for that person, too.

How will these freezes work? Contact all three of the nationwide credit reporting agencies – Equifax, Experian, and TransUnion. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee.

The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

For New Mexico Residents: You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of

removal pursuant to the Fair Credit Reporting and Identity Security Act. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

Fraud Alerts. A fraud alert tells businesses that check your credit that they should check with you before opening a new account. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

Federal Trade Commission and State Attorneys General Offices. 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 the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft. You may contact the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Maryland Residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For Texas Residents: You may contact and obtain information from your state attorney general at: Office of the Texas Attorney General www.texasattorneygeneral.gov/consumer-protection/identity-theft or contact the Identity Theft Hotline at 800-621-0508 (toll-free).

Reporting of identity theft and obtaining a police report.

You have the right to obtain any police report filed in the United States in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.