Orrick, Herrington & Sutcliffe LLP
401 Union Street - Suite 3300
Seattle, WA 98101
United States

+1 206-839-4300
orrick.com

June 26, 2023

By Email
attorneygeneral@doj.nh.gov

RE: Notice of Data Security Incident

Dear Attorney General:

We are writing on behalf of our client, Allegiant Air, LLC. ("Allegiant" or the "Company"), to notify you of a data security incident.

On May 31, 2023, Progress Software announced a previously unknown zero-day vulnerability in its MOVEit file transfer application, which is used by Allegiant and thousands of other enterprises around the world. On June 1, 2023, Allegiant identified evidence that an unauthorized third party used this vulnerability to gain access to the Company's MOVEit application, as part of a global attack on enterprises using the application. The Company immediately remediated the vulnerability and an investigation was launched with assistance from external cybersecurity experts. Allegiant also notified and is cooperating with law enforcement. On June 12, 2023, Allegiant determined that the event resulted in unauthorized download of employee personal information.

Allegiant determined that the personal information that was downloaded included

. The threat actor's motive appears to be part of a global scheme to extort enterprises for the return or deletion of the stolen data.

Allegiant is committed to safeguarding confidential and sensitive information. Allegiant has increased and added enhanced monitoring to its systems and continues to take steps to minimize the risk of this type of cyber event occurring in the future. Allegiant will also be undertaking a review of its security policies and procedures for potential enhancements.

The information of approximately one (1) New Hampshire resident was affected in the incident. The Company began notifying the resident via U.S. First Class Mail on June 26, 2023. A sample notice is attached as Attachment A.

If your office requires any further information in this matter, please contact me at .

Sincerely,

Aravind Swaminathan
Partner
Orrick, Herrington, & Sutcliffe, LLP

Attachment A - Sample Notice

Allegiant Air, LLC
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

[redacted]

June 26, 2023

Re: Notice of Data Breach

[redacted],

Allegiant Air, LLC ("Allegiant") recently experienced a cybersecurity event that involved some of your personal information. Please read this notice carefully, as it provides up-to-date information on what happened and what we are doing, as well as information on how you can obtain complimentary credit monitoring and identity restoration services.

What happened?

On May 31, 2023, a vendor of ours, Progress Software, announced a previously unknown vulnerability in its MOVEit file transfer application, which is used by Allegiant and thousands of other enterprises around the world. On June 1, 2023, Allegiant identified evidence that an unauthorized third party used this vulnerability to gain access to our MOVEit application, as part of a global attack on enterprises using the application. We use MOVEit to share and transfer files between Allegiant and vendors, government agencies, and individuals. We immediately remediated the vulnerability and an investigation was launched with assistance from external cybersecurity experts. We also notified law enforcement. We identified evidence that the unauthorized third party downloaded a number of files from our MOVEit application.

What information was involved?

Allegiant immediately began a process to determine who was affected and the types of information that were affected. This analysis was time consuming. On June 12, 2023, Allegiant determined that your personal information was downloaded, including: .

What we are doing:

Allegiant is committed to safeguarding confidential and sensitive information. Allegiant is offering two years of Triple Bureau Credit Monitoring/Triple Bureau Credit Report/Triple Bureau Credit Score/Cyber Monitoring services at no charge. These services provide you with alerts for twenty-four (24) months from the date of enrollment when changes occur to any of one of your Experian, Equifax or TransUnion credit files. This notification is sent to you the same day that the change or update takes place with the bureau. Cyber monitoring will look out for your personal data on the dark web and alert you if your personally identifiable information is found online. In addition, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

How do I enroll for the free services?

To enroll in Credit Monitoring services at no charge, please log on to **https://secure.identityforce.com/benefit/projectcedar** and follow the instructions provided. When prompted please provide the following unique code to receive services: [redacted]

In order for you to receive the monitoring services described above, **you must enroll by** . The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

In addition to immediately patching the vulnerability, Allegiant has increased and added enhanced monitoring to its systems and continues to take steps to minimize the risk of this type of cyber event occurring in the future. We will also be undertaking a review of our security policies and procedures for potential enhancements.

What you can do:

In addition to enrolling in the credit monitoring and identity restoration services being offered to you at no charge, we encourage you to take the following precautions:

- It is always a good idea to remain vigilant against threats of identity theft or fraud and to regularly review and monitor your account statements and credit history for any signs of unauthorized transactions or activity.
- if you ever suspect that you are the victim of identity theft or fraud, you can contact your local police. Additional information about how to protect your identity is contained in Attachment A.

For more information:

Allegiant has established a dedicated call center to answer questions about the security event as well as the credit monitoring and identity restoration services that we are offering to you. If you have any questions, please call the call center at between the hours of 8:00 a.m. to 8:00 p.m. Eastern Time, Monday through Friday and supply the representative with your unique code listed above.

Sincerely,

Daniel Creed
Chief Information Security Officer

Attachment A – Information for U.S. Residents

MORE INFORMATION ABOUT IDENTITY PROTECTION

INFORMATION ON OBTAINING A FREE CREDIT REPORT

U.S. residents are entitled under U.S. law to one free credit report annually from each of the three major credit bureaus. To order your free credit reports, visit www.annualcreditreport.com or call toll free +1 (877) 322 8228.

INFORMATION ON IMPLEMENTING A FRAUD ALERT OR SECURITY FREEZE

You can contact the three major credit bureaus at the addresses below to place a fraud alert on your credit report. A fraud alert indicates to anyone requesting your credit file that you suspect you are a possible victim of fraud. A fraud alert does not affect your ability to get a loan or credit. Instead, it alerts a business that your personal information might have been compromised and requires that business to verify your identity before issuing you credit. Although this may cause some short delay if you are the one applying for the credit, it might protect against someone else obtaining credit in your name.

A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing, or other services. A credit reporting agency may not charge you to place, temporarily lift, or permanently remove a security freeze.

To place a fraud alert or security freeze on your credit report, you must contact the three credit bureaus below:

Equifax	**Experian**	**TransUnion**
Consumer Fraud Division	Credit Fraud Center	TransUnion LLC
P.O. Box 740256	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022 2000
(888) 766 0008	(888) 397 3742	(800) 680 7289
www.equifax.com	www.experian.com	www.transunion.com

To request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, the addresses where you have lived over those prior five years;
5. Proof of current address such as a current utility bill or telephone bill; and
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.).

You may also contact the U.S. Federal Trade Commission ("FTC") for further information on fraud alerts, security freezes, and how to protect yourself from identity theft. The FTC can be contacted at 400 7th St. SW, Washington, DC 20024; telephone +1 (877) 382 4357; or www.consumer.gov/idtheft.

ADDITIONAL RESOURCES

Your state attorney general may also have advice on preventing identity theft, and you should report instances of known or suspected identity theft to law enforcement, your state attorney general, or the FTC.

Iowa Residents: The Attorney General can be contacted at Office of Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, Iowa 50319, +1 (515) 281-5164, www.iowaattorneygeneral.gov.

Maryland Residents: The Attorney General can be contacted at Office of Attorney General, 200 St. Paul Place, Baltimore, Maryland 21202; +1 (888) 743-0023; or www.marylandattorneygeneral.gov.

North Carolina Residents: The Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; +1 (877) 566-7226 (Toll-free within North Carolina); +1 (919) 716-6400; or www.ncdoj.gov.

New Mexico Residents: You have rights under the federal Fair Credit Reporting Act (FCRA), which governs the collection and use of information pertaining to you by consumer reporting agencies. For more information about your rights under the FCRA, please visit www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

New York Residents: The Attorney General can be contacted at the Office of the Attorney General, The Capitol, Albany, NY 12224-0341, +1 (800) 771-7755; or www.ag.ny.gov.

Oregon Residents: The Attorney General can be contacted at Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, +1 (877) 877-9392 (toll-free in Oregon), +1 (503) 378-4400, or www.doj.state.or.us.

For Arizona, California, Iowa, Montana, New York, North Carolina, Oregon, and Washington, 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).