

February 1, 2021

New Hampshire Office of the Attorney General
33 Capitol Street
Concord, NH 03301

STATE OF NH
DEPT OF JUSTICE
2021 FEB 16 PM 12:21

Re: Data Incident Notification

To Whom It May Concern:

I am writing on behalf of Jet Aviation Flight Services, Inc. ("Jet Aviation") pursuant to New Hampshire's data incident notification law to inform you of a data security incident. Jet Aviation provides various aviation services, including maintenance, aircraft charter, and aircraft management or staffing.

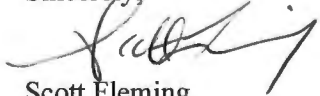
On December 23, 2020, Jet Aviation was informed by Avianis, our third-party scheduling software provider, of a data incident that has impacted Jet Aviation and other operators using the Avianis system. Avianis has notified Jet Aviation that on December 5, 2020, Avianis discovered unauthorized access to its network, which included personal information pertaining to Jet Aviation employees, contractors, and customers.

According to the information provided to us by Avianis, 32 New Hampshire residents for whom Jet Aviation is the data owner may have had their sensitive information affected by this incident. The scope of the incident may have included information such as full names and some combination of passport, travel visa, driver's license information and credit card information.

On December 29, 2020, Jet Aviation provided an e-mail notification of the incident to affected customers for whom Jet Aviation is the data owner, noting a general description of the incident, the personal information potentially impacted, and a contact information for further details. Furthermore, on or around February 10, 2021 the Jet Aviation will send notice by postal mail to those residents. A sample copy of the notice is enclosed. We also are working with Avianis to help prevent this type of incident from occurring again.

Please feel free to contact me if you have any questions or require additional information.

Sincerely,



Scott Fleming
Chief Legal Officer US
Scott.fleming@jetaviation.com

Enclosures: Email notification of the incident from Jet Aviation to affected customers and employees
Sample copy of the notice by postal mail to affected customers and employees

December 29, 2020

Re: Scheduling Software Data Incident

Dear Valued Customer,

We have recently been informed by Avianis, our third-party scheduling software provider, of a data incident. This incident has regrettably impacted Jet Aviation and a number of other operators using the system.

Our IT, Security and Operational Teams have been working closely with Avianis to ascertain the impact and determine next steps. At this stage, we understand certain categories of personally identifying data may have been compromised, notably passport, travel visa, and driver's license information. However, we do not believe that flight plans, passenger manifest details, and payment transactions have been compromised.

Avianis has notified local and Federal authorities of the incident and has assured us it will provide us with regular updates. Importantly, Avianis informed us it has identified and addressed the vulnerability that allowed this specific event to occur and has also informed us and other operators it has taken necessary corrective actions to prevent such an incident from occurring again.

We understand the importance of your privacy and deeply regret the inconvenience caused by this issue. Should you wish to subscribe to a monitoring service at this time, we will bear that cost.

We take such issues very seriously and will continue to keep you informed as we receive further updates from Avianis. In the meantime, please feel free to contact us directly. Alternatively, should you wish to reach one of our team, please contact your personal Client Aviation Director or send us an email at Data-Support@JetAviation.com.

Thank you for your understanding and continued loyalty.

Sincerely,



Leslie Cheshier
Vice President Owner & Charter Services US
+1 661 510 5111



Norbert Ehrich
Vice President Flight Services EMEA
+41 79 126 7680

February 1, 2021

Re: NOTICE OF DATA BREACH

Dear Customer

We are writing to inform you of a data security incident that may have affected personal information related to you. This notice describes what we know, steps we have taken in response to the incident, and additional actions you may wish to take to protect yourself.

WHAT HAPPENED?

On December 23, 2020, our third-party IT vendor, Avianis, notified us that there has been unauthorized access to its network on December 5, 2020 and potentially accessed information related to our customers and employees.

WHAT INFORMATION WAS INVOLVED?

Based on the information provided by the third-party IT vendor, it appears that information related to you may have been affected by this incident. Our IT, Security and Operational Teams have been working closely with Avianis to ascertain the impact and determine next steps. At this stage, we understand certain categories of personally identifying data may have been compromised, notably a combination of passport, travel visa, driver's license information, and credit card information.

WHAT WE ARE DOING

We regret this incident, and we take the privacy and security of your personal information very seriously. Avianis informed us it has identified and addressed the vulnerability that allowed this specific event to occur and has also informed us and other operators it has taken necessary corrective actions to prevent such an incident from occurring again.

WHAT YOU CAN DO

We know that the security of your personal information is important to you. As a precaution, we recommend that you remain vigilant to protect yourself. Please refer to Attachment 1 to this letter which provides additional information on those steps. Should you wish to subscribe to a monitoring service at this time, we will bear that cost. We have a preferential agreement with ID Watchdog for your consideration.

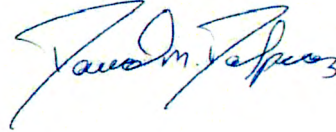
FOR MORE INFORMATION

Again, we regret any inconvenience this incident may cause. If you have any questions or need additional information, please contact your personal Client Aviation Director or send us an email at Data-Support@JetAviation.com.

Sincerely,



Leslie Cheshier
Vice President Owner & Charter Services US
4301 Empire Ave.
Burbank, CA 91505 / United States
+1 661 510 5111



David Dalpiaz
Vice President Flight Services US
113 Charles A. Lindbergh Drive
Teterboro, NJ 07608 / United States
+1 201 462 4126

Attachment 1: Additional Information

You should be cautious about using email to provide sensitive personal information, whether sending it yourself or in response to email requests. You should also be cautious when opening attachments and clicking on links in emails. Scammers sometimes use fraudulent emails or other communications to deploy malicious software on your devices or to trick you into sharing valuable personal information, such as account numbers, Social Security numbers, or usernames and passwords. The Federal Trade Commission (FTC) has provided guidance at <https://www.consumer.ftc.gov/articles/0003-phishing>.

You should review your financial statements and accounts for signs of suspicious transactions and activities. If you find any indication of unauthorized accounts or transactions, you should report the possible threat to local law enforcement, your State's Attorney General's office, or the FTC. You will find contact information for some of those entities below. If you discover unauthorized charges, promptly inform the relevant payment card companies and financial institutions. You may also have a right under state law to obtain a police report.

Fraud Alert Information

We recommend that you place a free "Fraud Alert" on your credit file. Fraud Alert messages notify potential credit grantors to verify your identification before extending credit in your name in case someone is using your information without your consent. A Fraud Alert can make it more difficult for someone to get credit in your name; however, please be aware that it also may delay your ability to obtain credit. Fraud alerts last one year. Identity theft victims can get an extended fraud alert for seven years.

Call only one of the following three nationwide credit reporting companies to place your Fraud Alert: TransUnion, Equifax, or Experian. As soon as the credit reporting company confirms your Fraud Alert, they will also forward your alert request to the other two nationwide credit reporting companies so you do not need to contact each of them separately. The contact information for the three nationwide credit reporting companies is:

Equifax	TransUnion	Experian
PO Box 740256	PO Box 2000	PO Box 9554
Atlanta, GA 30374	Chester, PA 19016	Allen, TX 75013
www.alerts.equifax.com	www.transunion.com/fraud	www.experian.com/fraud
1-800-525-6285	1-800-680-7289	1-888-397-3742

Free Credit Report Information

Under federal law, you are also entitled to one free credit report once every 12 months from each of the above three major nationwide credit reporting companies. Call 1-877-322-8228 or make a request online at www.annualcreditreport.com.

Even if you do not find any suspicious activity on your initial credit reports, we recommend that you check your account statements and credit reports periodically. You should remain vigilant for incidents of fraud

Jet Aviation Teterboro | Teterboro FBO

112 Charles A. Lindbergh Drive | Teterboro Airport | Teterboro, NJ 07608 | USA

Tel. +1 201 462 4000 | +1 800 538 0832 | Fax +1 201 462 4005 | www.jetaviation.com/teterboro

and identity theft. Victim information sometimes is held for use or shared among a group of thieves at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency or state attorney general and file a police report. Get a copy of the report; many creditors want the information it contains to alleviate you of the fraudulent debts. You also should file a complaint with the FTC using the contact information below. Your complaint will be added to the FTC's Consumer Sentinel database, where it will be accessible to law enforcers for their investigations.

You may also contact the FTC—or if you reside in Rhode Island, Maryland, or North Carolina, your state Attorney General's office—at the contact information below to learn more about identity theft and the steps you can take to protect yourself.

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue NW
Washington, DC 20580
1.877.FTC.HELP (382.4357)
www.ftc.gov/idtheft

Maryland Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023 www.marylandattorneygeneral.gov

Consumer Protection Division
NC Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
(919) 716- 6400 www.ncdoj.gov

Rhode Island Attorney General's Office
150 South Main Street
Providence, RI 02903
(401) 274-4400 www.riag.ri.gov

Security Freeze Information

You can request a free Security Freeze (aka "Credit Freeze") on your credit file by contacting each of the three nationwide credit reporting companies via the channels outlined below. When a credit Freeze is added to your credit report, third parties, such as credit lenders or other companies, whose use is not exempt under law will not be able to access your credit report without your consent. A Credit Freeze can make it more difficult for someone to get credit in your name; however, please be aware that it also may delay your ability to obtain credit.

Equifax Security Freeze
PO Box 105788
Atlanta, GA 30348
www.equifax.com/personal/credit-report-services/credit-freeze
1-800-349-9960

TransUnion Security Freeze
PO Box 2000
Chester, PA 19016
www.transunion.com/freeze
1-888-909-8872

Experian Security Freeze
PO Box 9554
Allen, TX 75013
www.experian.com/freeze
1-888-397-3742

To request a Credit Freeze, you may 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, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)