WILSON SONSINI

Wilson Sonsini Goodrich & Rosati
Professional Corporation
1700 K Street NW
Fifth Floor
Washington, D.C. 20006-3817
O: 202.973.8800
F: 202.973.8899

December 30, 2020

VIA US MAIL

Consumer Protection Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Security Incident

Dear Attorney General MacDonald,

We are writing on behalf of our client, Dassault Falcon Jet Corp., located at 200 Riser Road, Little Ferry, NJ 07643, and its subsidiaries (collectively, "Dassault Falcon Jet"), to inform you of a recent event that may affect the security of personal information of eleven New Hampshire residents who are current or former employees of Dassault Falcon Jet and certain of its subsidiaries, or their spouses and dependents.

Dassault Falcon Jet recently discovered ransomware on some of its systems and immediately took all systems offline, retained third-party cybersecurity experts to aid in its investigation, and worked to safely restore systems in a manner that protected the security of information on its systems. Dassault Falcon Jet sells, completes, and services high-quality business jets. Dassault Falcon Jet contacted the FBI and other appropriate law enforcement authorities and has and will continue to cooperate in any law enforcement investigation.

Dassault Falcon Jet's investigation identified evidence of unauthorized access to its systems by unknown persons. While the investigation is ongoing, Dassault Falcon Jet does not know if sensitive personal information held on its affected systems was in fact accessed.

On or about December 31, 2020, pursuant to N.H. Rev. Stat. Ann. § 359-C:20, Dassault Falcon Jet will begin mailing notification letters, in the same or substantially similar form as enclosed herein, to New Hampshire residents, which will include an offer of complimentary credit monitoring and fraud protection services for a period of twelve months.

Re: Notice of Data Security Incident
December 30, 2020

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

WILSON SONSINI GOODRICH & ROSATI
Professional Corporation

Allison J. Bender

Enclosure

DASSAULT FALCON JET

C/O IDX
P.O. Box 1907
Suwanee, GA 30024

To Enroll, Please Call:
833-754-1798
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code: [XXXXXXXX]

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

December 31, 2020

Notice of Data Breach

Dear <<First Name>> <<Last Name>>,

What Happened

This letter is to inform you that on December 6, 2020, Dassault Falcon Jet Corp. discovered a data security incident affecting some of our systems and some of our subsidiaries (collectively, "Dassault Falcon Jet" or "we"). Upon discovery of this security incident, we immediately took all affected systems offline and engaged third-party cybersecurity experts to aid in our investigation, as we work to safely restore our systems in a manner that protects the security of our personnel information. We also swiftly engaged law enforcement and will cooperate in any investigation they may pursue. Our investigation to-date has identified evidence of unauthorized access to systems from approximately June 19, 2020 to December 7, 2020 and potential unauthorized acquisition of some files containing information about you.

What Information Was Involved

The affected systems contained personal information regarding current and former employees of Dassault Falcon Jet, potentially including information regarding employees' spouses and dependents.

For current and former employees, the information involved includes name, personal and company email address, personal mailing address, employee ID number, driver's license number, passport information, financial account number, Social Security number, date of birth, work location, compensation and benefit enrollment information, and date of employment.

For information regarding current or former employees' spouses and dependents, the information involved may include name, address, date of birth, Social Security number, and benefit enrollment information. This does not include details of any claims, such as regarding health insurance.

What We Are Doing

We take the security of our personnel data very seriously. We are taking steps to investigate this incident and enhance our security program to help prevent similar incidents from happening in the future. Our intention is that each affected system will remain offline, until it can be restored with confidence in its safety and security. In a number of cases, we have rebuilt systems anew to maintain our operations while the investigation continues. As we restore and rebuild systems, we are also strengthening the security protections in place to protect those systems and the data stored on them.

In addition, we are offering identity theft protection services through IDX, a data breach and recovery services expert. IDX identity protection services include: 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do

We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling 833-754-1798 or going to https://app.idx.us/account-creation/protect and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is February 28, 2021.

We encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

For More Information

You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Please call 833-754-1798 or go to https://app.idx.us/account-creation/protect for assistance or for any additional questions you may have.

Sincerely,

Susan Wetzel

Susan Wetzel
VP, Human Resources

(Enclosure)

Recommended Steps to help Protect your Information

1. Website and Enrollment. Go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 833-754-1798 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, 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 Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer 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 a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

8. Regarding minors. Please note that credit monitoring services are not available for minor children because children typically do not have a credit file before 18 years of age, and as such, credit monitoring services generally are not considered a practical solution for minors. There are steps that you can take to protect your child's identity. Specifically, you can contact each of the credit reporting agencies to request a credit freeze for a minor child or a dependent, even if they do not have a credit report. To freeze a child's credit, a parent or guardian must submit required documentation to the three major credit bureaus, Equifax, Experian and TransUnion. Requests to freeze cannot be made online and must be mailed to each credit reporting agency directly.

- Equifax provides detailed information about freezing a child's credit on their website at https://www.equifax.com/personal/education/identity-theft/freezing-your-childs-credit-report-faq/, which provides this form, https://assets.equifax.com/assets/personal/Minor_Freeze_Request_Form.pdf.
- Experian provides detailed information about freezing a child's credit on their website at: https://www.experian.com/blogs/ask-experian/requesting-a-security-freeze-for-a-minor-childs-credit-report/#:~:text=The%20request%20can%20be%20mailed,file%20within%203%20business%20days, which provides this form, https://www.experian.com/freeze/form-minor-freeze.html.
- TransUnion provides information about freezing a credit file on their website at https://www.transunion.com/credit-freeze.

Copies of the following documents may be used to meet all three bureaus' requirements. It is recommended to make three sets of copies for each and not send originals:

- Your government-issued ID (usually a driver's license).
- Your birth certificate.
- Your child's birth certificate or other document showing you have the authority to act on the child's behalf (foster care certification, power of attorney or court order).

- **Your Social Security card.**
- **Your child's Social Security card.**
- **A utility bill or bank or insurance statement with your name and address on it.**

California Residents: The California Attorney General also provides guidance on ways to protect minors' information at: https://oag.ca.gov/idtheft/facts/freeze-child-credit.

All US Residents: The Federal Trade Commission also provides guidance on ways to protect minors' information at: https://www.consumer.ftc.gov/articles/0040-child-identity-theft#.