

FRESHFIELDS

TIMOTHY T. HOWARD

3 World Trade Center
175 Greenwich Street
New York, NY 10007

Tel +1 (212) 230-4690
timothy.howard@freshfields.com

October 18, 2024

Via Email (idtheft@oag.state.md.us)

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

To Attorney General Brown:

Pursuant to Md. Commercial Code § 14-3504(h), we are writing to inform you that Jet Aviation (Asia Pacific) Pte. Ltd. (the **Company**) is sending notices to Maryland residents advising them of a data incident.

On September 13, 2023, the Company became aware that a customer sent an invoice payment to the wrong bank account based on fraudulent wire instructions the customer received from a third party falsely purporting to be associated with the Company. The Company promptly initiated an investigation of the incident, discovered that a threat actor (**TA**) had obtained unauthorized access to the Company's systems, and immediately took steps to exclude the TA from the Company's systems, including by conducting a global password and token reset for all Company accounts, and blocking malicious domains identified as being associated with the TA.

The investigation revealed that the Company was the victim of a sophisticated business email compromise (**BEC**) fraud scheme that had the intent of diverting payments owed to the Company. Specifically, a third party obtained unauthorized access to five email accounts (including four individual email accounts, and one shared mailbox) to obtain invoices and then send fraudulent emails to a third party to divert an incoming payment due to the Company.

The Company promptly took steps to determine the scope of the incident and the data that may have been subject to unauthorized access, followed by a comprehensive review of the contents of that data. Although the shared mailbox was found to include personal information, the investigation revealed that it is highly unlikely that personal data was stolen or even accessed, because, among other things, evidence indicates that: (1) the TA's motive was to divert payments, consistent with a BEC scheme; (2) the shared mailbox did not contain targeted invoices; (3) the TA only accessed the shared mailbox on three occasions, and then diverted attention to, and focused attention on the individual mailboxes which contained such invoices and did not contain personal information for Maryland residents; and (4) the TA's identified manner of exfiltration was through manual email forwarding, which did not include emails from the shared mailbox.

However, in an abundance of caution the Company retained a third-party provider to review the unstructured data in the accounts, including the shared mailbox, to identify personal data that

stored in the accounts that could hypothetically have been accessed by the TA, even if such access was unlikely given the circumstances.

On September 18, 2024, that review revealed that hypothetically accessed data may have included certain personal information that would give rise to a notification obligation under Maryland law.

At this time, the Company has identified potentially affected records of personal information that correspond to five individuals who appear to be Maryland residents. By providing this notice, the Company does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

The data affected in this incident varies from person to person and includes some combination of the following: name, passport number and/or other government-issued identification number, and some health-related information, which the Company maintains in the ordinary course of business in its capacity as an airport and aircraft operator.

Commencing on October 18, 2024, a formal notice of the incident is being sent by U.S. mail to the individuals for whom the Company has identified a Maryland mailing address. A copy of the anticipated notice is attached.

The Company is not currently aware of any evidence indicating that the personal information involved in this incident has been misused in any manner that would cause harm to the impacted individuals. The Company's monitoring on the Internet, including the darkweb, has not detected the presence of any the potentially affected data. As noted above, consistent with a BEC scheme, all available evidence indicates that the scheme's primary purpose was to target invoice information to divert payments and was not concerned with obtaining personal information.

The Company takes the security, data privacy, and integrity of its customers' and employees' personal information seriously and maintains information technology measures designed to protect against unauthorized access to Company data. The Company is committed to the protection of the data it handles and will continue to confirm its safeguards and implement appropriate measures, as well as ensure employees are trained on responsible data handling practices.

Please contact me if you have any questions.

Sincerely,

/s/ Timothy T. Howard

Timothy T. Howard
Freshfields US LLP
3 World Trade Center
175 Greenwich Street, 51st Floor
New York, NY 10007
(212) 277-4000
timothy.howard@freshfields.com

Enclosure



Return Mail Processing
PO Box 999
Suwanee, GA 30024

1 1 1 *****SNGLP

SAMPLE A. SAMPLE - L01

APT ABC

123 ANY ST

ANYTOWN, US 12345-6789



October 18, 2024

Notice of Data Breach

We are writing to let you know about a data incident in which a third party may have gained unauthorized access to a limited amount of your personal information.

What Happened

On September 13, 2023, Jet Aviation (Asia Pacific) Pte. Ltd. (the **Company**) became aware that a limited number of Company email accounts had been subject to unauthorized access by a third party. We immediately took steps to restrict the unauthorized access and understand the scope of the incident, and successfully removed the third party's access to those email accounts and the Company's computer systems.

The investigation revealed that the incident was part of what is commonly referred to as a business email compromise (**BEC**) scheme, designed to divert a payment owed to the Company from another business. The Company also engaged resources to review the contents of the impacted email accounts to determine what data could have been potentially exposed by the incident. On September 18, 2024, that investigation revealed that one of these email accounts contained a limited amount of your personal information provided in connection with one or more flights into or out of Singapore.

There is no evidence that your information was actually viewed by the third party, and available evidence indicates that the third party was focused on stealing money owed to the Company rather than extracting any personal information. There is also no evidence that any of your personal information was exfiltrated from the Company's systems.

Even though there is no evidence that your personal information was improperly accessed, we are providing you this notice out of an abundance of caution.

Jet Aviation (Asia Pacific) Pte Ltd
Maintenance | Refurbishment | FBO
Maintenance Center
1071 West Camp Road
Seletar Aerospace Park
Singapore 797799

JetAviation.com
Tel. +65 6335 7335
Fax +65 6481 1480
Company Reg. No.: 197701894H

What Information Was Involved

The personal information that may have been accessed includes your name, [Extra1] that the Company maintains in the ordinary course of business.

What We Are Doing

The Company is committed to the protection of the data it handles and will continue to confirm its safeguards and implement appropriate measures, as well as ensure that employees are trained on responsible data handling practices. We have also implemented enhanced defensive measures to block unauthorized access to our corporate systems, and have not identified any further unauthorized activity since September 15, 2023. In addition, although we have no evidence that any personal information was improperly viewed or misused in a manner that could harm you, we are supporting those affected by offering a complimentary two-year membership of Experian's IdentityWorks. This product provides you with credit monitoring, identity theft detection, and resolution services. Please see Attachment A for instructions on how to enroll.

What You Can Do

In addition to complimentary credit monitoring, Attachment B provides further information about steps you can take to protect your identity in general, should you feel it is appropriate to do so.

For More Information

If you have any questions, you can call our dedicated toll-free telephone line at 1-833-918-5932, Monday through Friday from 8 am - 8 pm Central Time to speak to an authorized representative of the Company.

Yours sincerely,

Louis Leong
General Manager
Jet Aviation (Asia Pacific) Pte. Ltd.

Jet Aviation (Asia Pacific) Pte Ltd
Maintenance | Refurbishment | FBO
Maintenance Center
1071 West Camp Road
Seletar Aerospace Park
Singapore 797799

JetAviation.com
Tel. +65 6335 7335
Fax +65 6481 1480
Company Reg. No.: 197701894H

ATTACHMENT A

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for 24 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 24 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 24-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** January 31, 2025 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/credit
- 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 1-833-918-5932 by January 31, 2025. Be prepared to provide engagement number B133563 as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24-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 ExtendCARETM:** 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.

Jet Aviation (Asia Pacific) Pte Ltd
Maintenance | Refurbishment | FBO
Maintenance Center
1071 West Camp Road
Seletar Aerospace Park
Singapore 797799

JetAviation.com
Tel. +65 6335 7335
Fax +65 6481 1480
Company Reg. No.: 197701894H

ATTACHMENT B

GENERAL STEPS TO TAKE TO PROTECT YOUR PERSONAL INFORMATION

- You should be vigilant against possible “phishing” communications, including from emails that appear to be (but are not) sent from a particular organization.
- Regularly review your account statements and credit history for any signs of unauthorized transactions or activity, and remain vigilant against threats of identity theft or fraud.

STEPS YOU CAN TAKE TO PROTECT YOURSELF WITH REGARD TO CONSUMER CREDIT REPORTING BUREAUS

Ordering 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 at www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

Fraud Alert. When you place a “fraud alert” on your credit report, businesses who pull your credit report will see that you may be a victim of identity theft. The company may then choose to verify your identity before they extend credit to anyone who purports to be you. To place an alert, contact any one of the three main credit reporting bureaus. That company is required to tell the other two bureaus about the alert. When you first place a fraud alert on your account, it will remain for at least 90 days, after which you can renew it. When you do place an alert on your report, be sure that all three major credit reporting companies have your current contact information so they can get in touch with you.

Security Freeze. A “security freeze” or “credit freeze” goes further than an alert and lets you restrict access to your credit report entirely. This is because most creditors need to see your credit report before they approve a new account. If creditors cannot see your file, they may not extend the credit. A credit freeze does not affect your credit score, but you may need to lift the freeze temporarily, either for a specific time or for a specific party if you are opening a new account, applying for a job, renting an apartment or buying insurance.

To place a freeze, you need to contact each of the major credit reporting bureaus. You will need to supply your name, address, date of birth, social security number and other personal information. Credit reporting agencies are required to place/remove a freeze on your credit report without charge.

Below, we provide contact information for the major credit reporting agencies. They can provide additional resources about preventing or remedying identity theft, including by setting up fraud alerts/security freezes and by reviewing your credit report. Fees may be required for some services.

EQUIFAX
P.O. Box 105069
Atlanta, GA 30348-5069
866-478-0027
www.equifax.com/personal/credit-report-services

EXPERIAN
P.O. Box 9554
Allen, TX 75013
888-397-3742
www.experian.com/freeze

TRANSUNION
P.O. Box 160
Woodlyn, PA 19094
800-916-8800
freeze.transunion.com

Jet Aviation (Asia Pacific) Pte Ltd
Maintenance | Refurbishment | FBO
Maintenance Center
1071 West Camp Road
Seletar Aerospace Park
Singapore 797799

JetAviation.com
Tel. +65 6335 7335
Fax +65 6481 1480
Company Reg. No.: 197701894H

INFORMATION AND ASSISTANCE THAT YOU CAN OBTAIN FROM FEDERAL AND STATE LAW ENFORCEMENT AND CONSUMER PROTECTION AGENCIES:

If you believe that you may be the victim of identity theft, you should report that immediately to law enforcement, your state Attorney General, or the Federal Trade Commission. You also may wish to review the resources provided by the Federal Trade Commission on how to avoid identity theft. You can reach the FTC at:

Bureau of Consumer Protection
Federal Trade Commission
600 Pennsylvania Ave., NW
Washington, DC 20580

1-877-ID-THEFT (877-438-4338)
www.identitytheft.gov

PROTECTIONS OF THE FEDERAL FAIR CREDIT REPORTING ACT

The Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. In particular, the FCRA enables identity-theft victims to demand the removal of false entries on their credit reports that result from the theft. Your major rights under the FCRA include:

- 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.
- 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 reports to be provided to employers.
- You may limit “prescreened” offers of credit and insurance you get based on information in your credit report.
- You may seek damages from violators.

You can obtain more information, including information regarding additional rights at www.ftc.gov/credit, or at https://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.pdf.

IF YOU ARE A RESIDENT OF CERTAIN STATES, YOU HAVE ADDITIONAL RIGHTS:

MARYLAND

You can obtain information about steps you can take to avoid identity theft from the Attorney General. You can contact the Attorney General at:
200 St. Paul Place, 25th Floor
Baltimore, MD 21202
410-576-6491
<https://www.marylandattorneygeneral.gov/>

NORTH CAROLINA

You can obtain information about steps you can take to avoid identity theft from the Attorney General. You can contact the Attorney General at:
9001 Mail Service Center, Raleigh, NC 27699-9001
919-716-6400
<http://www.ncdoj.gov>

NEW YORK

You can contact the Attorney General at: 1-800-771-7755 and <https://ag.ny.gov/>. You can contact the New York Department of State, Division of Consumer Protection at 1-800-697-1220 and <https://dos.ny.gov/>. You can contact the Office of Information Technology Services at 844-891-1786 and <https://its.ny.gov/>.

RHODE ISLAND

You have the right to file or obtain a police report in regard to this incident. You can contact the Attorney General at 401-274-4400 and www.riag.ri.gov. One (1) Rhode Island resident was notified in connection with this incident.

Jet Aviation (Asia Pacific) Pte Ltd
Maintenance | Refurbishment | FBO
Maintenance Center
1071 West Camp Road
Seletar Aerospace Park
Singapore 797799

JetAviation.com
Tel. +65 6335 7335
Fax +65 6481 1480
Company Reg. No.: 197701894H