



Kamran Salour
650 Town Center Drive, Suite 1400
Costa Mesa, CA 92626
kamran.salour@lewisbrisbois.com
Direct: 714.966.3184

February 28, 2024

VIA EMAIL

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

Email: idtheft@oag.state.md.us

Re: Notification of Data Security Incident

To Whom It May Concern:

Lewis Brisbois represents King Aerospace in connection with a recent data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in accordance with Maryland data breach notification law.

1. Nature of the Security Incident

On or around December 5, 2023, King Aerospace discovered that it had experienced a cybersecurity incident. In response, King Aerospace took immediate steps to secure its digital environment and engaged cybersecurity experts to assist it with an investigation to determine what happened and identify whether any information may have been accessed or acquired without authorization. On January 22, 2024, King Aerospace learned that your personal information may have been impacted by the incident. Please note that there is no evidence of misuse or attempted misuse of any of the impacted information.

2. Type of Information and Number of Maryland Residents Affected

King Aerospace notified one (1) resident of Maryland of this data security incident via first class U.S. mail on February 28, 2024. The information accessed and potentially acquired by the unauthorized actor responsible for this incident may have included name and Social Security number. A sample copy of the notification letter sent to these individuals is included with this correspondence.

3. Steps Taken Relating to the Incident

King Aerospace also implemented measures to enhance the security of its digital environment in an effort to minimize the risk of a similar incident occurring in the future. Further, King Aerospace has offered all individuals whose information was involved twelve (12) months of complimentary services through TransUnion, which includes credit monitoring, dark web monitoring, a \$1 million identity fraud loss reimbursement policy, fully managed identity theft recovery services, and ninety (90) days access to a call center.

4. Contact Information

King Aerospace remains dedicated to protecting the personal information in its possession. If you have any questions or need additional information, please do not hesitate to contact me at (714) 966-3184 or by email at Kamran.Salour@lewisbrisbois.com.

Regards,

A handwritten signature in black ink, appearing to read 'Kamran Salour', with a stylized flourish at the end.

Kamran Salour of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Encl.: Sample Consumer Notification Letter

King Aerospace Inc.
c/o Cyberscout
1 Keystone Ave, Unit 700
Cherry Hill, NJ 08003
DB08555 4-4



[REDACTED]
[REDACTED]
[REDACTED]



February 28, 2024

Subject: Notice of Data Security Incident

Dear [REDACTED]:

We are writing to notify you of a recent data security incident our third-party vendor experienced that involved your personal information. We want to inform you of this incident and about steps you can take to help protect your personal information and offer you complimentary credit monitoring and identity protection services.

What Happened? On or around December 5, 2023, King Aerospace discovered that we had experienced a cybersecurity incident. In response, we took immediate steps to secure our digital environment and engaged cybersecurity experts to assist us with an investigation to determine what happened and identify whether any information may have been accessed or acquired without authorization. On January 22, 2024, we learned that your personal information may have been impacted by the incident. Please note that there is no evidence of misuse or attempted misuse of any of the impacted information.

What Information Was Involved? The impacted information may have included your name and Social Security number.

What Are We Doing? As soon as we discovered the incident, we took the steps described above. We also implemented measures to enhance the security of our digital environment in an effort to minimize the risk of a similar incident occurring in the future.

We are offering you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for twelve (12) months from the date of enrollment when changes occur to your credit file. This alert is sent to you the same day that a change or update takes place with the bureau. Finally, 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.

What Can You Do? We recommend that you review the guidance included with this letter about how to protect your personal information. In addition, we recommend enrolling in the complimentary services being offered by Cyberscout through Identity Force, a TransUnion company, to further protect your personal information. To receive credit monitoring services, you must be over the age of eighteen (18) and have established credit in the U.S., have a Social Security number to your name, and have a U.S. residential address associated with your credit file.

To enroll in Credit Monitoring services at no charge, please log on to <https://secure.identityforce.com/benefit/kingaero> 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 within 90 days from the date of this letter. 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.

For More Information. If you have any questions regarding the incident or would like assistance with enrolling in the services offered, please call 1-800-405-6108 between 8:00 am to 8:00 pm EST, Monday through Friday, excluding holidays.

We appreciate your understanding and deeply regret any worry or inconvenience that this may cause you.

Sincerely,

King Aerospace

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851 Atlanta, GA 30348-1
800-525-6285 www.equifax.com

Experian

P.O. Box 9532 Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 1000 Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General

Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
www.riag.ri.gov
1-401-274-4400

Washington D.C. Attorney General

441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.