



MULLEN
COUGHLIN LLC
ATTORNEYS AT LAW

RECEIVED

AUG 20 2018

CONSUMER PROTECTION

1275 Drummers Lane, Suite 302
Wayne, PA 19087

Ryan C. Loughlin
Office: 267-930-4786
Fax: 267-930-4771
Email: rloughlin@mullen.law

August 7, 2018

VIA U.S. MAIL

Attorney General Gordon J. MacDonald
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Security Incident

Dear Attorney General Gordon J. MacDonald,

We represent American Institute of Aeronautics and Astronautics (“AIAA”) located at 12700 Sunrise Valley Drive, Suite 200, Reston, Virginia, 20191-5807, and are writing to notify your office of an incident that may affect the security of some personal information relating to one (1) New Hampshire resident. By providing this notice AIAA does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about June 6, 2018, AIAA discovered suspicious emails sent to an employee. Upon discovery, AIAA immediately commenced an investigation. Third party forensic investigators were retained to assist with determining the nature and scope of the incident. It was discovered that the organization was the victim of a recent phishing attack beginning on or around the last week of May 2018. This attack was focused on capturing credentials to employee email accounts. The investigation determined that three employee email accounts were accessed without authorization between June 4, 2018 and June 6, 2018. Credentials for these three email accounts were changed to prevent further unauthorized access. The investigation also determined that search terms such as “invoice” and “wire transfer” were run in the accounts. A review of the contents of the three email accounts was undertaken to identify what information may have been accessible and who may be affected. This review determined that certain information related to certain individuals was included in emails that may have been viewed without authorization.

The information that may have been subject to unauthorized access includes name, bank or financial account number, and social security information.

Notice to New Hampshire Resident

On or about August 7, 2018, AIAA provided written notice of this incident to all affected individuals, which includes one (1) New Hampshire resident. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit A*.

Other Steps Taken and To Be Taken

Upon discovering the event, AIAA moved quickly to investigate and respond to the incident, assess the security of AIAA systems, and notify potentially affected individuals and applicable regulators. AIAA is also working to implement additional safeguards and training to its employees.

AIAA is providing access to credit monitoring, fraud consultation, and identity theft restoration services for two (2) years, through Kroll, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals. Additionally, AIAA is providing impacted individuals with guidance on how to protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. AIAA is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4786.

Very truly yours,



Ryan C. Loughlin of
MULLEN COUGHLIN LLC

RCL/alc
Enclosure

EXHIBIT A



<<Date>> (Format: Month Day, Year)

<<MemberFirstName>> <<MemberMiddleName>> <<MemberLastName>> <<Suffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<ZipCode>>

Notice of Data Breach

Dear <<MemberFirstName>> <<MemberLastName>>,

We write to inform you of a data privacy incident that could potentially affect the security of some of your personal information. We take this incident very seriously and are providing you with information and access to resources so that you can better protect your personal information, should you feel it is appropriate to do so.

What Happened? On or about June 6, 2018, we discovered suspicious emails sent to several employees. American Institute of Aeronautics and Astronautics (“AIAA”) immediately commenced an investigation and discovered that the organization was the victim of a recent phishing attack beginning on or around the last week of May 2018. This attack was focused on capturing credentials to employee email accounts. Third party forensic investigators were retained to assist with determining the nature and scope of the incident. The investigation determined that three employee email accounts were accessed without authorization between June 4, 2018 and June 6, 2018. Credentials for these three email accounts were changed to prevent further unauthorized access. The investigation also determined that search terms like “invoice” and “wire transfer” were run in the accounts. A review of the contents of the three email accounts was undertaken to identify what information may have been accessible and who may be affected. On or about July 6, 2018, it was determined that certain information related to you was included in emails that may have been viewed without authorization.

What Information Was Involved? Our investigation determined that the information related to you that was contained in the emails that may have been accessed includes: <<ClientDef1(data elements)>>

What We Are Doing. We have security measures, policies, and procedures in place to protect data in our care and we continue to review these measures as part of our ongoing commitment to the security of the information in our care. We are reporting this incident to applicable state and federal regulators as well as to the individuals who may be affected by this incident. We are also providing you with information about this event and about the steps you can take to better protect against misuse of your personal information, should you feel it appropriate to do so.

As an added precaution, we are also offering you access to two years of credit monitoring, fraud consultation, and identity theft restoration services through Kroll at no cost to you. The cost of this service will be paid for by AIAA. We encourage you to enroll in these services, as we are not able to act on your behalf to enroll you in the credit monitoring service.

Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit krollbreach.idMonitoringService.com to activate and take advantage of your identity monitoring services.

You have until **November 1, 2018** to activate your identity monitoring services.

Membership Number: <<Member ID>>


To receive credit services by mail instead of online, please call 1-844-263-8605. Additional information describing your services is included with this letter.

What You Can Do. Please review the enclosed "Steps You Can Take to Protect Your Information." You can also enroll to receive the free credit monitoring and identity theft protection services we are offering.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 1-866-775-4209 between 9 a.m. and 6 p.m. Eastern Time, Monday through Friday, excluding major U.S. holidays. Please have your membership number ready.

Again, AIAA takes the privacy and security of the personal information in our care seriously. We sincerely regret any inconvenience or concern this incident has caused you.

Sincerely,

A handwritten signature in black ink, appearing to read "Dan Dumbacher". The signature is fluid and cursive, with the first name "Dan" and last name "Dumbacher" clearly distinguishable.

Daniel L. Dumbacher
Executive Director

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Enroll in Credit Monitoring

Visit krollbreach.idMonitoringService.com to activate and take advantage of your identity monitoring services.

You have until **November 1, 2018** to activate your identity monitoring services.

Membership Number: <<Member ID>>

Monitor Your Accounts

Credit Reports. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your personal account statements and monitoring your free credit reports for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report. Contact information for the credit reporting agencies can be found below.

Fraud Alerts. At no charge, you can also have the three major credit bureaus place a “fraud alert” on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below:

Equifax
P.O. Box 105069
Atlanta, GA 30348
800-525-6285
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19106
800-680-7289
www.transunion.com

Security Freeze. You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer’s credit report without the consumer’s written authorization. However, please be advised 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. If you have been a victim of identity theft, and you provide the credit bureau with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. Fees vary based on where you live, but commonly range from \$3 to \$15. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. In order to request a security freeze, you will need to supply your full name, address, date of birth, Social Security number, current address, all addresses for up to five previous years, email address, a copy of your state identification card or driver’s license, and a copy of a utility bill, bank or insurance statement, or other statement proving residence. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
1-800-685-1111
www.freeze.equifax.com

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

TransUnion
P.O. Box 2000
Chester, PA 19016
1-888-909-8872
freeze.transunion.com

Additional Information. You can further educate yourself regarding identity theft, security freezes, fraud alerts, and the steps you can take to protect yourself against identity theft and fraud by contacting the Federal Trade Commission or your state Attorney General, as well as the credit reporting agencies listed above. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission encourages those who discover that their information has been misused to file a complaint with them. You have the right to file a police report if you ever experience identity theft or fraud, and instances of known or suspected identity theft should be reported to law enforcement. Please note that in order to file a police 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. This notice has not been delayed as the result of a law enforcement investigation.

For Maryland residents, the Maryland Attorney General can be reached at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and www.oag.state.md.us.

For North Carolina residents, the North Carolina Attorney General can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; by phone toll-free at 1-877-566-7226; by phone at 1-919-716-6400; and online at www.ncdoj.gov.

For 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 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. We encourage you to 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.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following Kroll identity monitoring services¹ for a period of two years beginning on the date you activate the services. Please note, you have until November 1, 2018 to activate your identity monitoring services.

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

¹ Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.