



MULLEN  
COUGHLIN<sub>LLC</sub>  
ATTORNEYS AT LAW

STATE OF NH  
DEPT OF JUSTICE

2018 FEB 13 AM 10:35

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

1275 Drummers Lane, Suite 302  
Wayne, PA 19087

February 9, 2018

**INTENDED FOR ADDRESSEE(S) ONLY**

**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 Event**

Dear Attorney General MacDonald:

We represent the Connecticut Airport Authority ("CAA"), 334 Ella Grasso Turnpike, Windsor Locks, CT 06096, and are writing to notify your office of an incident that may affect the security of personal information relating to one (1) New Hampshire resident. The investigation into this incident is ongoing, and this notice will be supplemented with any substantive information learned after submission of this notice. By providing this notice, CAA 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 November 14, 2017, CAA learned of phishing emails being sent from certain CAA employees' Outlook email accounts. Although CAA immediately changed the employees' email account credentials, CAA discovered on November 15, 2017, additional employees received the prior phishing email. CAA immediately launched an internal investigation, including retaining the services of a third party forensic investigation firm to assist in determining what happened. Although the investigation is ongoing, CAA has determined that certain CAA employees were victims of a phishing attack that resulted in these credentials being used by unknown individual(s) to access their CAA Outlook email account. CAA has not identified any other suspicious activity occurring within the email accounts other than the unauthorized transmission of phishing emails.

**Notice to New Hampshire Resident**

While the investigation is ongoing, CAA confirmed after a review of the contents of the email accounts that the first and last name and financial account information relating to one (1) New Hampshire resident

may have been accessible to the unauthorized individual(s). CAA is providing written notice of this incident to those impacted by this incident, including one (1) New Hampshire resident on or about February 9, 2018, in substantially the same form as the letter attached hereto as *Exhibit A*.

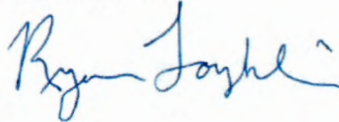
#### **Other Steps Taken and To Be Taken**

CAA is providing impacted individuals access to twenty-four (24) months of complimentary credit monitoring and identity restoration services with Kroll, and has established a dedicated toll-free number for individuals to contact with questions or concerns regarding this incident. Additionally, CAA is providing these individuals with helpful information on how to protect against identity theft and fraud, including how to place a fraud alert and security freeze on one's credit file, the contact information for the national consumer reporting agencies, 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, state attorney general, and law enforcement to report attempted or actual identity theft and fraud. CAA is also providing notice of this incident to other state regulators as required.

#### **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,

A handwritten signature in blue ink that reads "Ryan Loughlin". The signature is written in a cursive style with a small flourish at the end.

Ryan C. Loughlin of  
MULLEN COUGHLIN LLC

# **EXHIBIT A**



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

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

## Re: Notice of Data Privacy Event

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

The Connecticut Airport Authority ("CAA") are writing to inform you of a recent incident that may impact the security of your personal information. We are writing to ensure that you are aware of the incident so that you may take steps to protect your personal information should you feel it is appropriate to do so.

**What Happened?** On or about November 14, 2017, CAA learned of phishing emails being sent from certain CAA employees' email accounts. CAA immediately began to investigate this email activity and quickly changed the credentials for these accounts. A third party forensic investigation firm was retained to assist in determining what happened and what information may be contained in the email accounts. The ongoing investigation has determined that certain CAA employees were victims of a phishing attack that resulted in unauthorized access to their email accounts. We have not identified any other suspicious activity occurring within the email accounts other than the unauthorized transmission of phishing emails but are unable to rule out access to any particular email or attachment in the account.

**What Information was Involved?** We determined on December 29, 2017, that the following information relating to you was contained in one of the impacted email accounts at the time of this incident: <<ClientDef1(first and last name; [Insert Data Elements])>>.

**What We Are Doing?** The confidentiality, privacy, and security of information in our care is one of our highest priorities. When we discovered this incident, we immediately took steps to terminate the unauthorized access, determine how this event occurred, and confirm what personal data may have been at risk as a result of this incident.

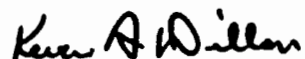
To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for two years. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

In addition to providing this notice to you and access to the free identity monitoring services listed above, we have been reviewing our existing policies and procedures, providing additional training on phishing emails and working with our third-party forensic investigation team to ensure the security of our systems. We will also be providing notice to certain state Attorneys General and consumer reporting agencies as required.

**What You Can Do.** You can review the enclosed *Steps You Can Take to Protect Against Identity Theft and Fraud*, which contains instructions on how to enroll and receive free credit monitoring and identity restoration services, as well as information on what you can do to better protect yourself against the possibility of identity theft and fraud should you feel it is appropriate to do so.

**For More Information.** We sincerely regret any inconvenience or concern this may have caused. We understand you may have questions that are not answered in this letter. To insure your questions are answered in a timely manner, please contact Kroll at 1-866-775-4209, Monday through Friday from 9:00 a.m. to 6:00 p.m. Eastern Standard Time.

Sincerely,

A handwritten signature in black ink that reads "Kevin A. Dillon". The signature is written in a cursive style with a large, stylized initial "K".

Kevin A. Dillon, A.A.E.  
Executive Director, Connecticut Airport Authority

Encl.



## Steps You Can Take to Protect Against Identity Theft and Fraud

Visit [krollbreach.idMonitoringService.com](http://krollbreach.idMonitoringService.com) to activate and take advantage of your identity monitoring services.

You have until **May 10, 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.

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. 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](http://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.

At no charge, you can also have these 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](http://www.equifax.com)

Experian  
P.O. Box 2002  
Allen, TX 75013  
888-397-3742  
[www.experian.com](http://www.experian.com)

TransUnion  
P.O. Box 2000  
Chester, PA 19022-2000  
800-680-7289  
[www.transunion.com](http://www.transunion.com)

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, list 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. 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. 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](http://www.freeze.equifax.com)

Experian Security Freeze  
P.O. Box 9554  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com/freeze/center.html](http://www.experian.com/freeze/center.html)

TransUnion  
P.O. Box 2000  
Chester, PA 19022-2000  
1-888-909-8872  
[www.transunion.com/credit-freeze](http://www.transunion.com/credit-freeze)

You can further educate yourself regarding identity theft, fraud alerts, and the steps you can take to protect yourself, by contacting the Federal Trade Commission or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; [www.identitytheft.gov](http://www.identitytheft.gov); 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. You have the right to file a police report if you ever experience identity theft or 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 they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed by law enforcement. **For Maryland residents**, the 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](http://www.oag.state.md.us).

**For North Carolina residents**, the Attorney General can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; toll-free at 1-877-566-7226; by phone at 1-919-716-6400; and online at [www.ncdoj.gov](http://www.ncdoj.gov). **For Rhode Island residents**, the Attorney General can be contacted by mail at 150 South Main Street, Providence, RI 02903; by phone at (401) 274-4400; and online at [www.riag.ri.gov](http://www.riag.ri.gov). A total of 1 Rhode Island resident(s) may be impacted by this incident.

**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](http://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. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above.



## TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services<sup>1</sup> from Kroll:

### **Triple Bureau Credit Monitoring**

You will receive alerts when there are changes to your credit data at any of the three national credit bureaus—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.

<sup>1</sup> 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.