



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

RECEIVED

MAR 16 2020

CONSUMER PROTECTION

Sian M. Schafle  
Office: (267) 930-4799  
Fax: (267) 930-4771  
Email: [sschafle@mullen.law](mailto:sschafle@mullen.law)

1275 Drummers Lane, Suite 302  
Wayne, PA 19087

March 12, 2020

**VIA U.S. MAIL**

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

**Re: Notice of Data Event**

Dear Sir or Madam:

We represent Greater Washington Educational Telecommunications Association, Inc. (“WETA”) located at 3939 Campbell Avenue, Arlington, VA 22206, and are writing to notify your office of an incident that may affect the security of some personal information relating to three (3) New Hampshire residents. This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, WETA 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**

WETA recently became aware of unusual activity relating to a limited number of WETA employee and consultant email accounts. WETA immediately commenced an investigation with the assistance of third-party computer specialists. The investigation determined that these email accounts were accessed without authorization at varying times between March 20, 2019 and December 31, 2019. While the investigation did not determine that personal information had been viewed by an unauthorized actor, WETA could not rule out the possibility of such activity. Therefore, in an abundance of caution, WETA immediately began a thorough review of the contents of the email accounts to determine whether sensitive information was present at the time of the incident.

WETA received the preliminary results of the investigation on February 3, 2020; those results indicated that personal information may have been present in the affected email account at the time of the incident. However, the results contained false positives and missing address information and, therefore, required the review of relevant source documents, review of internal records, and working with an outside vendor to confirm the last known address for potentially affected individuals and to confirm whether the information was protected under relevant laws.

WETA confirmed that the information that could have been subject to unauthorized access includes personal information as defined by N.H. Rev. Stat. Ann. § 359-C:19(IV) such as name, address, and Social Security number.

#### **Notice to New Hampshire Residents**

On March 12, 2020, WETA began providing written notice of this incident to affected individuals, which includes three (3) New Hampshire residents. 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, WETA moved quickly to investigate and respond to the incident, assess the security of WETA systems, and notify potentially affected individuals. Specifically, WETA immediately changed the credentials for the involved email accounts. As part of WETA's ongoing commitment to the security of information, WETA is also reviewing and enhancing existing policies and procedures to reduce the likelihood of a similar future event. WETA is providing access to credit monitoring and identity protection services for one year through Kroll, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, WETA is providing impacted individuals with guidance on how to better 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. WETA is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, 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) 930-4799.

Very truly yours,



Sian M. Schafle of  
MULLEN COUGHLIN LLC

Enclosure  
SMS/ras

# EXHIBIT A



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

<<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>  
<<address\_1>>  
<<address\_2>>  
<<city>>, <<state\_province>> <<postal\_code>>  
<<country >>

**Re: Notice of Data Privacy Event**

Dear <<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>,

Greater Washington Educational Telecommunications Association, Inc. ("WETA") is writing to inform you of an incident that may affect the security of some of your personal information. While there is currently no evidence that your information has been misused as a result of this incident, out of an abundance of caution, we are providing you with information about the incident, our response, and resources available to you to help protect your information should you feel it appropriate to do so.

**What Happened?** WETA recently became aware of unusual activity relating to a limited number of WETA employee and consultant email accounts. We immediately commenced an investigation with the assistance of third-party computer specialists. The investigation determined that these email accounts were accessed without authorization at varying times. While the investigation did not determine that personal information had been viewed by an unauthorized actor, WETA could not rule out the possibility of such activity. Therefore, we immediately began a thorough review of the contents of the email accounts to determine whether sensitive information was present at the time of the incident. Through this process, we determined that your personal information was present in at least one of the involved email accounts from <<b2b\_text\_2 (Breach Date Range)>>.

**What Information Was Involved?** The investigation determined that at the time of the incident, the following types of your personal information were present in at least one of the involved email accounts: your <<b2b\_text\_1 (Impacted Data)>>. To date, we are not aware of any actual or attempted misuse of your personal information in relation to this incident.

**What We Are Doing.** WETA takes the confidentiality, privacy, and security of information in its care very seriously. While WETA has security measures in place to protect information in its care, we are also taking steps to implement additional safeguards and review WETA policies and procedures in order to ensure we protect the security of information on our systems. Specifically, WETA immediately changed the credentials for the involved email accounts.

As an added precaution, WETA is providing you with access to twelve months of identity monitoring services from Kroll at no cost to you. A description of services and instructions on how to enroll can be found within the enclosed *Steps You Can Take to Help Protect Personal Information*. Please note that you must complete the enrollment process yourself, as we are not permitted to enroll you in these services on your behalf.

**What You Can Do.** You can review the enclosed *Steps You Can Take to Help Protect Personal Information*. You can also enroll to receive the free identity monitoring services through Kroll.

## **Additional Information**

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, 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); TTY: 1-866-653-4261. 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. 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 report with law enforcement for identity theft, you will likely need to provide some proof that you 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.



## **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 Chrome, Firefox, Safari and Edge. 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.

## STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

### **Enroll in Credit Monitoring and Identity Theft Restoration Services**

Additional information describing the services provided to you is included with this letter.

Visit <https://enroll.idheadquarters.com> to activate and take advantage of your identity monitoring services.

You have until **June 19, 2020** to activate your identity monitoring services.

Membership Number: <<Member ID>>

### **Monitor Your Accounts**

In addition to enrolling in the complimentary services detailed above, we encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements and explanation of benefits, and to monitor your credit reports for suspicious activity and 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](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.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

#### **Experian**

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 160

Woodlyn, PA 19094

1-888-909-8872

[www.transunion.com/credit-freeze](http://www.transunion.com/credit-freeze)

#### **Equifax**

PO Box 105788

Atlanta, GA 30348-5788

1-800-685-1111

[www.equifax.com/personal/credit-report-services](http://www.equifax.com/personal/credit-report-services)

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

#### **Experian**

P.O. Box 9554

Allen, TX 75013

1-888-397-3742

[www.experian.com/fraud/center.html](http://www.experian.com/fraud/center.html)

#### **TransUnion**

P.O. Box 2000

Chester, PA 19016

1-800-680-7289

[www.transunion.com/fraud-victim-resource/place-fraud-alert](http://www.transunion.com/fraud-victim-resource/place-fraud-alert)

#### **Equifax**

P.O. Box 105069

Atlanta, GA 30348

1-888-766-0008

[www.equifax.com/personal/credit-report-services](http://www.equifax.com/personal/credit-report-services)

**For More Information.** We understand you may have questions about this incident that are not addressed in this letter. If you have questions or concerns, please call our dedicated hotline at 1-844-968-1705, Monday through Friday, from 9:00 a.m. to 6:30 p.m. Eastern Time, excluding national holidays. You may also write to WETA at 3939 Campbell Avenue, Arlington, VA 22206.

Sincerely,

A handwritten signature in black ink, appearing to read 'D. Purvis', written in a cursive style.

David C. Purvis  
Senior Vice President and Chief Financial Officer  
WETA