



Lindsay B. Nickle
2100 Ross Avenue, Suite 2000
Dallas, Texas 75201
Lindsay.Nickle@lewisbrisbois.com
Direct: 214.722.7141

File No. 49905.52

February 22, 2022

VIA ELECTRONIC MAIL

Attorney General Brian E. Frosh
Office of the Attorney General
Attn: Security Incident Notification
200 St. Paul Place
Baltimore, MD 21202
Email: ldtheft@oag.state.md.us

Re: **Notice of Data Security Incident**

Dear Attorney General Frosh:

Lewis Brisbois Bisgaard & Smith LLP ("Lewis Brisbois") represents North Texas Public Broadcasting ("KERA"), a national radio station based out of Dallas, Texas, in connection with a recent data security incident that may have affected the information of certain Maryland residents. This letter is being sent in pursuant to Md. Code Ann. Com m. Law 14-3504. The incident in question is described in further detail below.

1. Nature of the Security Incident

KERA experienced a network disruption on September 17, 2021, when KERA discovered that certain files on its systems were encrypted by an unknown actor. Upon becoming aware of this, KERA immediately took all systems offline to help contain the incident and engaged an independent computer forensics firm to determine the scope of the incident and whether personal information was acquired without authorization. KERA undertook a review of the information that could have potentially been accessed in connection with the incident. October 14, 2021, KERA determined that information related to its former and current employees was potentially impacted. These individuals were notified through U.S. First-Class Mail on November 19, 2021.

Additionally, the initial investigation led to a more thorough review of potentially compromised data by the forensics firm. On December 9, 2021, additional individuals were identified whose information may have been accessed without authorization. KERA then diligently worked to identify complete and accurate address information to notify these individuals. On January 25, 2022, the additional individuals were notified through U.S. First-Class Mail. The information on the Maryland resident may have included name, address, and social security number. To date, KERA has no evidence that any potentially impacted information has been misused in conjunction with this incident.

2. Number of Maryland Residents Affected

KERA notified one (1) Maryland resident of this data security incident via U.S. First-Class Mail on January 25, 2022. A sample copy of the notification letter sent to the affected individual is included in this letter.

3. Steps Taken Relating to the Incident

KERA implemented additional security measures to reduce the risk of a similar incident occurring in the future and to protect the privacy and security of all personal information in its possession. Specifically, since the incident occurred, KERA has completed the following:

- 1.) Reset passwords for all employees and systems;
- 2.) Migrated email from Microsoft Exchange server to Office 365;
- 3.) Deployed multi-factor authentication and single sign on software for all end user devices;
- 4.) Installed additional cybersecurity software on all end user devices, internal file server and equipment along with 24/7 third-party security monitoring; and
- 5.) Rebuilt internal file server using zero-trust model.

In addition, KERA has offered complimentary identity monitoring services through Kroll to the notified individuals. KERA has also established a toll-free call center through Kroll to answer any questions about the incident and address related concerns. The call center is available Monday through Friday from 8:30 a.m. to 5:30 p.m. Central Time, excluding some U.S. holidays.

4. Contact Information

KERA remains dedicated to protecting the personal information in its control. If you have any questions or need additional information, please do not hesitate to contact me at 214.722.7141 or via email at Lindsay.Nickle@lewisbrisbois.com.

Very truly yours,



Lindsay B. Nickle of
LEWIS BRISBOIS BISGAARD & SMITH LLP

LBN/sas
Encl: Sample Consumer Notification Letter



<<MemberFirstName>> <<MemberLastName>>

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

<<Address1>>

<<Address2>>

<<City>>, <<State>> <<Zip Code>>

Notice of Data Breach

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

We are writing to tell you about a data security incident that may have exposed some of your personal information. We take the protection and proper use of your information very seriously. For this reason, we are contacting you directly to explain the circumstances of the incident.

What happened?

On September 17, 2021, KERA discovered that certain files on its systems were encrypted by an unknown actor. Upon discovering this, KERA immediately began an investigation and took all systems offline to help contain the incident. KERA engaged an independent computer forensics firm to determine what happened and whether personal information had been acquired without authorization. Before the forensic investigation concluded, KERA identified one file containing personal information that may have been accessed/acquired without authorization. KERA learned this on October 14, 2021, and notified all individuals identified in this specific file. On December 9, 2021, the forensics firm concluded its investigation and determined that additional information, including some of your information, was impacted by the incident.

What information was involved?

The information compromised included your <variable field>.

What we are doing.

As soon as we discovered this incident, we took the steps described above. We have also implemented additional safeguards to help ensure the security of our network to reduce the risk of a similar event occurring in the future.

In addition, 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 one year. 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, Web Watcher, Public Persona, Quick Cash Scan, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit <<IDMonitoringURL>> to activate and take advantage of your identity monitoring services.

You have until <<Date>> to activate your identity monitoring services.

Membership Number: <<Member ID>>

Additional information describing your services is included with this letter.

What you can do.

Please review the enclosed “Additional Resources” section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

For more information.

If you have questions, please call 1-???-???-????, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time. Please have your membership number ready.

Protecting your information is important to us. We trust that the services we are offering to you demonstrate our continued commitment to your security and satisfaction.

Sincerely,

A handwritten signature in black ink that reads "Nico Leone". The signature is written in a cursive, flowing style.

Nico Leone

Chief Executive Officer

KERA – North Texas Public Broadcasting

STEPS YOU CAN TAKE TO FURTHER 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.

IRS Identity Protection PIN: You can obtain an identity protection PIN (IP PIN) from the IRS that prevents someone else from filing a tax return using your Social Security number. The IP PIN is known only to you and the IRS and helps the IRS verify your identity when you file your electronic or paper tax return. You can learn more and obtain your IP PIN here: <https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>.

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

Texas Attorney General

PO Box 12548
Austin, TX 78711
texasattorneygeneral.gov/consumer-protection
1-800-621-0508

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>.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

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 will be able to help you determine if it is an indicator of identity theft.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you will receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You will receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

\$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to \$1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

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 will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

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.