



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Rebecca J. Jones
Office: (267) 930-4839
Fax: (267) 930-4771
Email: rjones@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

January 28, 2022

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

Dear Sir or Madam:

We represent Internews Network (“Internews”) located at PO 4448, Arcata, CA 95518, and are writing to notify your office of an incident that may affect the security of some personal information relating to one hundred twenty-four (124) Maryland residents. This notice may be supplemented with new significant facts learned subsequent to its submission. By providing this notice, Internews does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On December 7, 2021, Internews became aware of possible activity related to certain computer systems. Internews immediately launched an investigation, with the assistance of third-party forensic specialists, to determine the full nature and scope of the activity and to secure its network. That investigation, which took several weeks to conclude, determined that there was unauthorized access to Internews systems between October 2015 and December 2021. As a result, the unauthorized actor had access to and may have acquired information regarding certain individuals whose information was located within the affected systems. Although the investigation found no evidence that there actually was any unauthorized access to or acquisition of any individual’s personal information, Internews conducted a thorough review of the relevant systems to identify the types of information stored within them and to whom this information related. On or about January 3, 2022, Internews’ review determined that the involved systems contained protected information related to certain individuals.

The information that could have been subject to unauthorized access includes name, Social Security number, and date of birth.

Notice to Maryland Residents

On or about January 28, 2022, out of an abundance of caution, Internews began providing written notice of this incident to all affected individuals, which includes one hundred twenty-four (124) Maryland 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, Internews moved quickly to investigate and respond to the incident, assess the security of Internews systems, and notify potentially affected individuals. Internews is also working to implement additional safeguards and training to its employees. Internews is providing access to credit monitoring 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, Internews is providing impacted individuals with guidance on how to better protect against identity theft and fraud. Internews 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) 930-4839.

Very truly yours,

Rebecca J. Jones of
MULLEN COUGHLIN LLC

RJJ:bwt
Enclosure

Exhibit *A*



Internews
Local voices. Global change.

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

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

RE: <<b2b_text_1(SubjectLine)>>

Dear <<first_name>> <<last_name>>:

Internews Network ("Internews") writes to notify you of an incident that may affect the privacy of some of your information. Although we do not have evidence to suggest that your information was viewed or used by another party, we take this incident seriously. This letter provides details of the incident, our response, and steps you may take to protect against possible misuse of your personal information, should you feel it appropriate to take extra precautions. We know that this may be unsettling. We have arranged for a dedicated phone number you can call if you have questions, and are also sharing information about resources and support that you can start using today if you choose.

What Happened? On December 7, 2021, Internews became aware of possible activity related to certain computer systems. We immediately launched an investigation, with the assistance of third-party forensic specialists, to determine the nature and scope of the activity. That investigation, which took several weeks to conclude, determined that we were subject to a cyber event, and there was unauthorized access to our systems between October 2015 and December 2021.

What Information Was Involved? We conducted a thorough, detailed review of the affected systems to understand the nature and extent of the intrusion and determined that systems storing employee information could have been accessed. While we have no reason to believe that the unauthorized access resulted in any information related to you being viewed or taken, we are making you aware of this incident out of an abundance of caution. We have no reason to believe that any identity theft or unauthorized use of the affected information has occurred. For your reference, the information contained in the impacted systems that could possibly have been accessed, although we have no evidence of that, includes your <<b2b_text_2(DataElements)>>.

What is Internews Doing? Upon discovery, we immediately commenced an investigation to confirm the nature and scope of the incident and worked to secure our network. We have also taken steps to implement additional monitoring and safeguards and to review our policies and procedures relating to data privacy and security.

Internews is providing you with access to twenty-four (24) months of identity services through Kroll at no cost to you. A description of services and instructions on how to activate can be found within the enclosed *Steps You Can Take to Help Protect Against Identity Theft and Fraud*. Please note that you must complete the activation process yourself, as we are not permitted to activate these services on your behalf.

What You Can Do. You can review the enclosed *Steps You Can Take to Help Protect Against Identity Theft and Fraud*. You can also activate the complimentary identity services through Kroll, which is included in the following pages. We also 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.

For More Information. If you have additional questions about this incident, please contact 1-855-568-2167, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays.

Internews takes the privacy and security of the information in our care seriously. We sincerely regret any inconvenience or concern this incident may cause you.

Sincerely,

Office of the Chief Operating Officer
Internews Network

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

Activate Identity Monitoring

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.

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

You have until **<<b2b_text_6(ActivationDeadline)>>** to activate your identity monitoring services.

Membership Number: **<<MembershipNumber(S_N)>>**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

If you prefer to activate these services offline and receive monitoring alerts via the US Postal Service, you may activate via our automated phone system by calling 1-888-653-0511, Monday through Friday, 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. Please have your membership number located in your letter ready when calling. Please note that to activate monitoring services, you will be required to provide your name, date of birth, and Social Security number through our automated phone system.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services 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 will 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.

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.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit 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 three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit 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 credit 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 credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to 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.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may 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 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 and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th St. NW, Washington, D.C. 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us. Internews Network is located at PO 4448, Arcata, CA 95518.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 2 Rhode Island residents 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 bureaus 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.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov/>.