

Clausen, Elsa

From: Anne R. Noble <anoble@alhurra.com>
Sent: Thursday, February 16, 2023 2:53 PM
To: Consumer
Subject: Notification of Cyber Attack
Attachments: 58920-middle-east-broadcasting-networks-mailer-02-16-2023_11-37-04-58920.pdf;
58920-middle-east-broadcasting-networks-mailer-02-16-2023_11-37-04-58920
_Insert.pdf

You don't often get email from anoble@alhurra.com. [Learn why this is important](#)

February 16, 2023

Sent via Email and Certified Mail

Office of the Attorney General of Maryland

Consumer Protection Division

200 St. Paul Place

Baltimore, MD 21202

*Re: Middle East Broadcasting Networks. Inc., 7600 Boston Blvd,
Springfield, VA 22153*

To Whom It May Concern:

On February 4, 2023, Middle East Broadcasting Networks, Inc. ("MBN") discovered that its computer systems had been compromised by a cyber-attack. MBN immediately interrupted further incursion by disabling its internet service. To date, that service remains disabled, as experts engaged by MBN assess and document the damage and secure all systems. MBN

is working closely with the FBI and with the cyber-security team at the United States Agency for Global Media (the independent federal agency that provides MBN with one hundred percent of its funding.)

MBN believes that certain information stored in its systems, including documents containing the names, Social Security numbers, and home addresses of current and former staff and contractors, was accessed by the criminals behind the cyber-attack. MBN will begin expedited notification of all current and former staff members and contractors who may have been impacted by the cyber-attack, in order to provide them with more detailed information about what occurred and with tools for safeguarding their information. Many are also receiving two years of credit-monitoring, paid for by MBN. For reference, please find, attached, the notification letter to be sent to MBN's Maryland employees. MBN leadership notified current staff last week, and conducted a virtual town-hall meeting with an extensive question-and-answer session on Tuesday. The undersigned is available to staff to answer additional queries.

The number of Maryland residents (including current and former employees and individual contractors) potentially affected by the attack is 499.

MBN takes this data breach seriously and is committed to fully securing its systems, preventing a recurrence, and protecting the privacy of all of its employees and contractors.

Please contact me directly by email (anoble@alhurra.com) or telephone (703-852-9040) should you have additional questions or concerns.

Very truly yours,

Anne R. Noble, Esq.

General Counsel

Anne Noble
General Counsel



Middle East Broadcasting Networks, Inc.
7600 Boston Blvd
Springfield, VA 22153
T: +1 703-852-9040 | M: +1 202-299-7465
anoble@alhurra.com

This electronic mail (e-mail) transmission is meant solely for the person(s) to whom it is addressed. It contains confidential information that may also be legally privileged. Any copying, dissemination or distribution of the contents of this e-mail by anyone other than the addressee or his or her agent is strictly prohibited. If you have received this e-mail in error, you are directed to notify me immediately by telephone, facsimile and/or e-mail and to purge the original and all copies thereof. Thank you. Internet communications are not assured to be secure or clear of inaccuracies as information could be intercepted, corrupted, lost, destroyed, arrive late or incomplete, or contain viruses. Therefore, we do not accept responsibility for any errors or omissions that are present in this email, or any attachment, that have arisen as a result of e-mail transmission

<Date>

Notice of Data Breach

|||||

Recipient's Name

Address 1

Address 2

Dear <First><Last>,

We are writing to inform you of an incident involving your personal information. The intent of this letter is to share what we know, what we are doing to address it, and to provide some information and resources for steps you can take to protect your personal information.

What Happened

On February 4, 2023, MBN discovered that its computer systems had been compromised by a cyber attack. MBN immediately engaged the services of a cybersecurity vendor to determine the extent of the incursion. At the same time, MBN interrupted further incursion by disabling its internet service. This remains disabled while a comprehensive survey is completed by the vendor. All efforts have been conducted in close coordination with the United States Agency for Global Media (MBN's grantor) and their cyber security team, as well as the FBI.

What Information Was Involved

The data involved may have included your Social Security number and home address.

What We Are Doing

After detecting the intrusion, MBN quickly initiated preventative measures to restrict additional data loss. We are implementing additional safeguards to enhance data security and are taking additional steps to protect against criminal activity in the future.

In addition, we are offering identity theft protection services through Norton LIFELOCK. LIFELOCK identity protection services include: credit monitoring, identity monitoring, and automated alerts if a problem is detected. With this protection, Norton LIFELOCK will help you resolve issues if your identity is compromised.

We thus wanted to make you aware of these events and provide you with information about how to protect yourself.

What You Can Do

We encourage you to enroll in the free identity protection services MBN is offering. To do so, please follow the instructions sent to you by LIFELOCK, which will be sent to you directly by LIFELOCK in a separate letter.

We also encourage you to periodically check your credit reports to ensure that no fraudulent activity has occurred. Even if there are no signs of fraud on these reports, we recommend that you remain vigilant, continue to check these credit reports and your account statements periodically, and report anything suspicious to law enforcement.

Please read the attachment to this letter to review recommendations from the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert and/or security freeze on your credit file.

At this time, MBN has no evidence that your information has been misused. However, we encourage you to take full advantage of all available services.

For More Information

Keeping your personal information secure is of the utmost importance to MBN. We sincerely regret any concern or inconvenience this event may cause you. Should you have any questions regarding this letter, please contact me at anoble@alhurra.com (please put Security Concern in the subject line of your email).

Thank you for your time and attention to this important matter.

Middle East Broadcasting Networks, Inc.

Recommended Steps to Help Protect Your Information

- 1. Website and Enrollment.** Please follow the instructions in the letter sent to you directly by LIFELOCK.
- 2. Activate the credit monitoring** provided as part of your LIFELOCK identity protection membership. The monitoring included in the membership must be activated to be effective.
- 3. Review your credit reports.** We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

You should also know that you have the right to file a police report if you ever experience identity 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 you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

4. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting 1-866-349-5191 P.O. Box 105069 Atlanta, GA 30348-5069 www.equifax.com	Experian Fraud Reporting 1-888-397-3742 P.O. Box 9554 Allen, TX 75013 www.experian.com	TransUnion Fraud Reporting 1-800-680-7289 P.O. Box 2000 Chester, PA 19022-2000 www.transunion.com
--	--	---

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

5. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

6. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

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 a 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. You can 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.

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

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.