BakerHostetler

Baker&Hostetler LLP

312 Walnut Street
Suite 3200
Cincinnati, OH 45202-4074

T 513.929.3400
F 513.929.0303
www.bakerlaw.com

Joseph L. Bruemmer
direct dial: 513.929.3410
jbruemmer@bakerlaw.com

March 31, 2022

VIA E-MAIL (DOJ-CPB@DOJ.NH.GOV)

Attorney General John Formella
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Incident Notification

Dear Attorney General Formella:

We are writing on behalf of our client, Sinclair Broadcast Group, Inc. ("Sinclair"), to notify your office of a cybersecurity incident. Sinclair's headquarters are located at 10706 Beaver Dam Road, Hunt Valley, Maryland 21030.

On October 17, 2021, Sinclair determined that certain devices in its network had been encrypted with ransomware. Sinclair immediately began an investigation, a cybersecurity firm was engaged, and measures were taken to address the incident and to restore the systems. Sinclair also notified law enforcement and is supporting its investigation. The evidence showed that there was unauthorized activity in Sinclair's network between June 23, 2021, and October 17, 2021. The evidence also showed that there was unauthorized access to files on its file servers. Sinclair carefully reviewed these files and, on March 4, 2022, determined that one or more of the files contained the name and Social Security number of two New Hampshire residents.

On March 31, 2022, Sinclair will mail notification letters to the New Hampshire residents in accordance with N.H. Rev. Stat. Ann. § 359-C:20[1], via United States First-Class mail. A copy of the notification letter is enclosed. Sinclair is offering the New Hampshire residents a complimentary one-year subscription to identity monitoring services through IDX. A dedicated, toll-free call center has been established for individuals to call with questions about the incident.

[1] This report does not waive Sinclair's objection that New Hampshire lacks regulatory authority over it related to any claims that may arise from this incident.

To help prevent something like this from happening again, Sinclair is taking steps to enhance already existing security measures by, among other things, implementing enhanced network monitoring tools.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

Joseph L. Bruemmer
Partner

Enclosure

Sinclair Broadcast Group
Return to IDX
10300 SW Greenburg Rd. Suite 570
Portland, OR 97223

To Enroll, Please Call:
1-800-939-4170
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code: <<XXXXXXXX>>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

March 31, 2022

Dear <<First Name>> <<Last Name>>,

Sinclair Broadcast Group, Inc. ("Sinclair") understands the importance of protecting information. We are writing to inform you that we recently identified and addressed a security incident that involved some of your information. This notice explains the incident, outlines the measures we have taken in response, and provides some additional steps you can take.

On October 17, 2021, we determined that certain devices in our network had been encrypted with ransomware. We immediately began an investigation, a cybersecurity firm was engaged, and measures were taken to address the incident and to restore the systems. We also notified law enforcement and are supporting its investigation.

The evidence showed that there was unauthorized activity in our network between June 23, 2021, and October 17, 2021. The evidence also showed that there was unauthorized access to files on our file servers. We carefully reviewed these files and, on March 4, 2022, determined that one or more of the files contained your name and <<variable text>>.

As a precaution, we are offering you credit monitoring and identity protection services through the company IDX at no cost to you. These identity protection services include one year of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. These services are completely free to you, and enrolling in this program will not hurt your credit score. **For more information on the services, including instructions on how to activate your complimentary one-year membership, please visit https://app.idx.us/account-creation/protect or call 1-800-939-4170 and use the Enrollment Code provided above. Please note the deadline to enroll is June 30, 2022**. For more information on identity protection and steps you can take in response, please see the additional information provided with this letter.

We take your trust in us and this matter very seriously. To help prevent something like this from happening again, we are taking steps to enhance our existing security measures by, among other things, implementing enhanced network monitoring tools. If you have any questions, please call 1-800-939-4170, Monday through Friday, between 9:00 a.m. and 9:00 p.m. Eastern Time.

Sincerely,

Sinclair Broadcast Group, Inc.

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information.
After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

If your health insurance or medical information was involved: It is always advisable to review any statements you may receive from your health insurer or healthcare providers. If you see charges for services that you did not receive, contact your insurer or provider immediately.

Sinclair Broadcast Group, Inc. is located at 10706 Beaver Dam Road, Hunt Valley, Maryland 21030 and can be reached at 410.568.1500.

Additional information for residents of the following states:

Maryland: You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.oag.state.md.us

New York: You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection*, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotection; and *New York State Office of the Attorney General*, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov

North Carolina: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov

Rhode Island: This incident involves 2 individuals in Rhode Island. Under Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov