McDonald Hopkins
A business advisory and advocacy law firm®

McDonald Hopkins PLC
39533 Woodward Avenue
Suite 318
Bloomfield Hills, MI 48304

P 1.248.646.5070
F 1.248.646.5075

Dominic A. Paluzzi
Direct Dial: 248.220.1356
E-mail: dpaluzzi@mcdonaldhopkins.com

January 28, 2022

VIA U.S. MAIL

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

Re: ALM Media Properties, LLC – Incident Notification

Dear Mr. Formella:

McDonald Hopkins PLC represents ALM Media Properties, LLC ("ALM"). I am writing to provide notification of an incident at ALM that may affect the security of personal information of approximately one (1) New Hampshire resident. ALM's investigation is ongoing, and this notification will be supplemented with any new or significant facts or findings subsequent to this submission, if any. By providing this notice, ALM does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

ALM detected anomalous network activity and discovered that it had experienced a malware incident that infected a number of its systems and encrypted files on several machines. Upon learning of the issue, ALM promptly opened an investigation. As part of its investigation, ALM immediately launched an investigation in consultation with outside cybersecurity professionals who regularly investigate and analyze these types of situations to analyze the extent of any compromise of its network. ALM's investigation determined that between March 31, 2021 and May 12, 2021, in addition to encrypting files, an unauthorized party removed a limited number of files and folders from its system. ALM then worked to identify what personal information, if any, might have been present in those files. After a complex analysis of those files, ALM discovered on January 4, 2022 that the impacted files included the affected resident's full name and financial account number.

To date, ALM is not aware of any reports of identity fraud or improper use of any information as a direct result of this incident. Nevertheless, out of an abundance of caution, ALM wanted to inform you (and the affected resident) of the incident and to explain the steps that it is taking to help safeguard the affected resident against identity fraud. ALM is providing the affected resident with written notification of this incident commencing on or about January 28, 2022 in substantially the same form as the letter attached hereto. ALM will advise the affected resident to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. ALM will advise the affected resident about the process for

placing a fraud alert and/or security freeze on their credit files and obtaining free credit reports. The affected resident is also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

At ALM, protecting the privacy of personal information is a top priority. ALM is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. ALM continually evaluates and modifies its practices to enhance the security and privacy of the personal information it maintains.

Should you have any questions regarding this notification, please contact me at (248) 220-1356 or dpaluzzi@mcdonaldhopkins.com. Thank you for your cooperation.

Sincerely,

Dominic A. Paluzzi

Encl.

ALM Media Properties, LLC

[redacted]

[redacted]

[redacted]

[redacted]

Dear [redacted],

We are writing with important information regarding a recent security incident. The privacy and security of the personal information we maintain is of the utmost importance to ALM Media Properties, LLC ("ALM"). We wanted to provide you with information about the incident and let you know that we continue to take significant measures to protect your information.

What Happened?

We detected anomalous network activity and discovered that we had experienced a malware incident that infected a number of our systems and encrypted files on several machines. As soon as we learned of the abnormal activity, we immediately took steps to secure our environment and data.

What We Are Doing.

Upon learning of the issue, in addition to taking the remediation and restoration steps above, we commenced an immediate and thorough investigation. As part of our investigation, we engaged external cybersecurity professionals experienced in handling these types of incidents. Our investigation concluded that between March 31, 2021 and May 12, 2021, in addition to encrypting files, an unauthorized party removed a limited number of files and folders from our system. We then worked to identify what personal information, if any, might have been present in those files. After a complex analysis of those files, we discovered on January 4, 2022 that the impacted files contained some of your personal information.

What Information Was Involved?

The impacted files contained some of your personal information, specifically your [redacted]. **Your Social Security number was not contained in the files.**

What You Can Do.

We have no indication or evidence that any of that data has been or will be misused. Nevertheless, out of an abundance of caution, we want to make you aware of the incident.

This letter provides precautionary measures that you can take to protect your personal information, including placing a fraud alert and/or security freeze on your credit files, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

For More Information.

Please accept our sincere apologies that this incident occurred. We are committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at [redacted]. The response line is staffed with professionals familiar with this incident and knowledgeable on what you can do if you are concerned about potential misuse of your information. **The response line is available Monday through Friday, 9 a.m. to 9 p.m. ET.**

Sincerely,

ALM Media Properties, LLC

– OTHER IMPORTANT INFORMATION –

1. Placing a Fraud Alert on Your Credit File.

We recommend that you place an initial one-year "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax
P. O. Box 105788
Atlanta, GA 30348
https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
1-800-525-6285

Experian
P. O. Box 9554
Allen, TX 75013
https://www.experian.com/fraud/center.html
1-888-397-3742

TransUnion
P. O. Box 6790
Fullerton, CA 92834-6790
https://www.transunion.com/fraud-alerts
1-800-680-7289

2. Consider Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
https://www.equifax.com/personal/credit-report-services/credit-freeze/
1-800-349-9960

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
http://experian.com/freeze
1-888-397-3742

TransUnion Security Freeze
P.O. Box 2000
Chester, PA 19016
https://www.transunion.com/credit-freeze
1-888-909-8872

In order to place the security freeze, 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 reporting company will send you a confirmation letter containing 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.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the City in which you currently reside.

3. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

4. **Additional Helpful Resources.**

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If this notice letter states that your financial account information and/or payment card information was impacted, we recommend that you contact your financial institution to inquire about steps to take to protect your account, including whether you should close your account or obtain a new account number.

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: 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.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 1-877-566-7226.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; https://ag.ny.gov/consumer-frauds-bureau/identity-theft; Telephone: 1-800-771-7755.

Washington D.C. Residents: You may obtain information about preventing identity theft from the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Suite 110 South, Washington D.C. 2001, https://oag.dc.gov/consumer-protection, Telephone: 1-202-727-3400.

Oregon Residents: You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 1-877-877-9392.