

Spencer S. Pollock, CIPP/US, CIPM
Direct Dial: 1.410.456.2741
Cell: 1.410.917.5189
Email: spollock@mcdonaldhopkins.com

January 4, 2023



VIA EMAIL (Idtheft@oag.state.md.us)

Brian E. Frosh
Office of the Attorney General
St. Paul Plaza
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Affiliated Management – Incident Notification

Dear Mr. Frosh:

McDonald Hopkins PLC represents Affiliated Management, Inc. (“Affiliated Management”). I am writing to provide notification of an incident at Affiliated Management that may affect the security of personal information of approximately (4) four Maryland residents. Affiliated Management’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, Affiliated Management does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

Affiliated Management recently learned that an unauthorized individual may have obtained access to an employee email account on or around November 15, 2022. Affiliated Management 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 the email accounts and the security of the emails and attachments contained within them. Affiliated Management devoted considerable time and effort to determine what information was contained in the affected email accounts. Based on its comprehensive investigation and document review, Affiliated Management discovered that the compromised email accounts contained a limited amount of personal information, including the affected residents’ full names, Social Security numbers, and driver’s license numbers. On December 30, 2022, Affiliated Management confirmed the most recent contact information of the potentially impacted individuals.

To date, Affiliated Management 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, Affiliated Management is providing the affected residents with written notification of

Spencer S. Pollock, CIPP/US, CIPM
Direct Dial: 1.410.456.2741
Cell: 1.410.917.5189
Email: spollock@mcdonaldhopkins.com

January 4, 2023

VIA EMAIL (Idtheft@oag.state.md.us)

Brian E. Frosh
Office of the Attorney General
St. Paul Plaza
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202



Re: Affiliated Management – Incident Notification

Dear Mr. Frosh:

McDonald Hopkins PLC represents Affiliated Management, Inc. (“Affiliated Management”). I am writing to provide notification of an incident at Affiliated Management that may affect the security of personal information of approximately (4) four Maryland residents. Affiliated Management’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, Affiliated Management does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

Affiliated Management recently learned that an unauthorized individual may have obtained access to an employee email account on or around November 15, 2022. Affiliated Management 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 the email accounts and the security of the emails and attachments contained within them. Affiliated Management devoted considerable time and effort to determine what information was contained in the affected email accounts. Based on its comprehensive investigation and document review, Affiliated Management discovered that the compromised email accounts contained a limited amount of personal information, including the affected residents’ full names, Social Security numbers, and driver’s license numbers. On December 30, 2022, Affiliated Management confirmed the most recent contact information of the potentially impacted individuals.

To date, Affiliated Management 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, Affiliated Management is providing the affected residents with written notification of

January 4, 2023

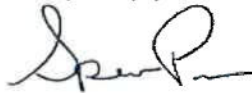
Page 2

this incident commencing on or about January 5, 2022 in substantially the same form as the letter attached hereto. Affiliated Management is offering the affected residents complimentary one-year memberships with a credit monitoring service. Affiliated Management is advising the affected residents about the process for placing fraud alerts and/or security freezes on their credit files and obtaining free credit reports. The affected residents are being advised to contact their financial institutions to inquire about steps to take to protect their accounts. The affected residents are also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

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

If you have any additional questions, please contact me at (410) 456-2741 or spollock@mcdonaldhopkins.com.

Very truly yours,



Spencer S. Pollock

Encl.

Affiliated Management, Inc.
c/o Cyberscout



IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY

Re: Data Security Incident

Dear [REDACTED]

At Affiliated Management, Inc., we take the protection of your personal information very seriously. We also strongly believe in transparency which is why, as a precautionary measure, we are writing with important information regarding a data security incident that may involve your protected personal information, what we did in response, and steps you can take to protect yourself against possible misuse of the information.

What Happened?

On or about November 15, 2022, we discovered suspicious activity in one of our employee email accounts involving funds misdirected to a fraudulent account. At that time, we acted quickly to secure the account and conduct an investigation into the incident.

At the conclusion of our preliminary investigation, we determined that an unauthorized actor likely gained access to protected personal information. We conducted further review and on December 12, 2022, we concluded our review and determined that the impacted data may have contained some of your protected personal information.

We are not aware of any misuse of any information, however, we wanted to notify you of the incident out of an abundance of caution and provide you with information on how to best protect your identity.

What We Are Doing.

Upon learning of the incident, we commenced a prompt and thorough investigation. We immediately took steps to investigate any potential unauthorized access to email accounts. As part of our investigation, we have worked very closely with external cybersecurity professionals.

What Information Was Involved?

The types of information involved included your first and last name, Social Security number and driver's license.

What You Can Do.

To protect you from potential misuse of your information, we are providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you



P18HFA00300001000010102GG0500

with alerts for twelve months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

This letter also provides other precautionary measures 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.

We sincerely regret this incident occurred and for any concern it may cause. We understand that you may have questions about it beyond what is covered in this letter. If you have any further questions regarding this incident, please contact [REDACTED] between the hours of 8:00 am to 8:00 pm Eastern time, Monday through Friday, excluding holidays.

Sincerely,

[REDACTED]

Affiliated Management, Inc.

[REDACTED]

- OTHER IMPORTANT INFORMATION -

Website and Enrollment To enroll in Credit Monitoring services at no charge, please log on to <https://secure.identityforce.com/benefit/affiliatedmanagement> and follow the instructions provided. When prompted please provide the following unique code to receive services: [REDACTED] In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.



Activate the credit monitoring provided as part of your Cyberscout identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, Cyberscout will be able to assist you.

Placing a Fraud Alert

Whether or not you choose to use the complimentary 12-month credit monitoring services, we recommend that you place an initial 90-day "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 105069
Atlanta, GA 30348-5069
<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>
(800) 525-6285

Experian

P.O. Box 9554
Allen, TX 75013
<https://www.experian.com/fraud/center.html>
(888) 397-3742

TransUnion

Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19016-2000
<https://www.transunion.com/fraud-alerts>
(800) 680-7289

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 cost. 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 sending a request in writing, by mail, to all three nationwide credit reporting companies. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348-5788
<https://www.equifax.com/personal/credit-report-services/credit-freeze/>
(888)-298-0045

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
<http://experian.com/freeze>
(888) 397-3742

TransUnion Security Freeze

P.O. Box 160
Woodlyn, PA 19094
<https://www.transunion.com/credit-freeze>
(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 you do place a security freeze prior to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

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.

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 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.

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: 888-743-0023.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain a police report in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

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: 800-771-7755.

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: 877-566-7226 (Toll-free within North Carolina), 919-716-6000.

Washington D.C. Residents: You may obtain information about preventing identity theft from the Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington D.C. 20001, <https://oag.dc.gov/consumer-protection>, Telephone: 202-442-9828.