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

May 10, 2023

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

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

Re: ActivCare Living – Incident Notification

Dear Mr. Brown:

McDonald Hopkins PLC represents ActivCare Living. I am writing to provide notification of an incident at ActivCare Living that may affect the security of personal information of approximately two (2) Maryland residents. ActivCare Living'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, ActivCare Living does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

On or about April 13, 2023, ActivCare detected unauthorized access to some of the data maintained on the ActivCare Orange web-based portal of their payroll service provider. Upon learning of the unauthorized access, ActivCare Living immediately commenced an internal investigation. On or about April 27, 2023, ActivCare Living discovered the information that may have been accessed potentially contained some personal information including individual's Social Security Number, bank account with routing number, and insurance or benefit information.

Upon learning of this issue, ActivCare Living immediately commenced an internal investigation and promptly notified potentially affected individuals. ActivCare Living wanted to inform you (and the affected residents) of the incident and to explain the steps that it is taking to help safeguard the affected residents against identity fraud. ActivCare Living is providing the affected residents with written notification of this incident commencing on or about May 11, 2023 in substantially the same form as the letter attached hereto. ActivCare Living is offering residents complimentary one-year membership with a credit monitoring service. ActivCare Living will advise the affected residents to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. ActivCare Living will advise the affected residents about the process for placing a fraud alert and/or security freeze on their credit files and obtaining free credit reports. The affected residents are also being provided with the contact information for the consumer reporting agencies, the Federal Trade Commission and the Maryland Attorney General.

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

If you have any additional questions, please contact me at (248) 220-1356 or dpaluzzi@mcdonaldhopkins.com.

Very truly yours,

Dominic A. Paluzzi

Encl.

ActivCare Living
c/o Cyberscout
1 Keystone Ave., Unit 700
Cherry Hill, NJ 08003
DB-07462

[redacted]

[redacted]

IMPORTANT INFORMATION PLEASE REVIEW CAREFULLY

Dear [redacted]:

At ActivCare Living, we take the protection of your personal information very seriously. We also strongly believe in transparency which is why, we are writing with important information regarding a data security incident that may involve your information. We want to provide you with information about the incident, inform you about the services we are providing to you, and let you know that we continue to take significant measures to protect your information.

<u>What Happened?</u>

On or about April 13, 2023, ActivCare detected unauthorized access to some of the data maintained on the ActivCare Orange web-based portal of our payroll service provider.

<u>What We Are Doing.</u>

Upon learning of the unauthorized access, we immediately contained the environment and commenced an internal investigation. Following the completion of our investigation, it was determined that some information may have been accessed by the unauthorized actors. On or about April 27, 2023, we discovered the information that may have been accessed potentially contained some of your personal information.

<u>What Information Was Involved?</u>

The information that may have been accessed contained some of your personal information, including [redacted].

<u>What You Can Do.</u>

To date, we have no evidence that your information has or will be misused. However, out of an abundance of caution, we are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services <u>at no charge to you</u>. These services provide you with alerts for 12 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.

How do I enroll for the free services?

To enroll in Credit Monitoring services at no charge, please log on to [redacted] 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.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering.

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 understand that you may have questions beyond what is covered in this letter. Representatives are available for 90 days from the date of this letter to assist you with questions regarding this incident, between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays. Please call the help line [redacted] and supply the fraud specialist with your unique code listed above.

We sincerely regret this incident occurred and for any concern or inconvenience it may have caused.

Sincerely,

ActivCare Living
9619 Chesapeake Drive, Suite 103
San Diego, CA 92123

– OTHER IMPORTANT INFORMATION –

1. 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

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 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.

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.

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.