

James J. Giszczak
Direct Dial: 248-220-1354
E-mail: jgiszczak@mcdonaldhopkins.com

January 12, 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: DPP II, LLC – Incident Notification

Dear Attorney General Frosh:

McDonald Hopkins PLC represents DPP II, LLC dba Home Care Providers of Texas (“HCPT”). I am writing to provide notification of an incident at HCPT that may affect the security of personal information of one (1) Maryland resident. By providing this notice, HCPT does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

On June 29, 2022, HCPT learned that its network had been affected by a cyberattack that encrypted certain files maintained on the network. Upon learning of this issue, HCPT contained the threat by disabling and isolating the affected systems, and immediately began a prompt and thorough investigation. As part of the investigation, HCPT worked very closely with external cybersecurity experts experienced in handling these types of incidents. After an extensive forensic investigation and comprehensive review of all the data impacted, on November 15, 2022, HCPT discovered that the unauthorized party accessed certain files containing personal information that were maintained on the affected systems. The information potentially accessed include full name, Social Security number, and driver license number or state ID.

HCPT has no indication that any of the information has been used for identity theft or financial fraud. Nevertheless, out of an abundance of caution, HCPT 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. HCPT is providing the affected resident with written notification of this incident commencing on or about January 12, 2023 in substantially the same form as the letter attached hereto. HCPT is also offering the affected resident complimentary one-year membership with a credit monitoring service. HCPT will advise the affected resident to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. HCPT will advise the affected resident about the process for placing a

January 12, 2023

Page 2

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 HCPT, protecting the privacy of personal information is a top priority. HCPT is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. HCPT 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) 220-1354 or jgiszczak@mcdonaldhopkins.com.

Very truly yours,



James J. Giszczak

Encl.

Homecare Providers of Texas
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998



January 12, 2023

IMPORTANT INFORMATION - PLEASE REVIEW CAREFULLY

Dear [REDACTED]:

The privacy of your personal information is of utmost importance to Home Care Providers of Texas ("HCPT"). As a current or former employee of HCPT, we are writing to provide you with important information about a recent incident which involves the security of some of your personal information that was maintained by us. We want to provide you with information regarding the incident, and explain the services we are making available to help safeguard your information against potential identity fraud. We also are providing additional steps you can take to further protect your information.

What Happened?

On June 29, 2022, HCPT learned that our network had been affected by a cyberattack that encrypted certain files maintained on our network.

What We Are Doing.

Upon learning of this issue, we contained the threat by disabling and isolating the affected systems, and immediately began a prompt and thorough investigation. As part of our investigation, we worked very closely with external cybersecurity experts experienced in handling these types of incidents. We also notified law enforcement and appropriate state and federal regulatory agencies about the incident. After an extensive forensic investigation and comprehensive review of all the data impacted, on November 15, 2022, we discovered that certain personal information maintained on our systems was potentially accessed by an unauthorized party between June 15, 2022 and June 29, 2022.

What Information Was Involved?

The potentially accessed information may include your full name, address, social security number, and driver license information.

Please be assured, at this time, HCPT has no evidence that information involved in this incident has been used for identity theft or financial fraud.

What You Can Do.

To protect your information, we are providing you access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for twelve (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 the event that you become a victim of fraud.

000010102G0500

P

These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services. This service is completely free to you, and enrolling in this program will not hurt your credit score. For more information on identity theft prevention, including instructions on how to activate your complimentary twelve (12) months - membership, please see the additional information provided in this letter.

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 any credit files, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and monitoring your free credit reports for fraudulent or irregular activity on a regular basis.

Please accept our apology that this incident occurred. We are committed to maintaining the privacy of your information and have taken many precautions to help safeguard it. We continually evaluate and modify our practices to enhance the security and privacy of the personal information in our possession, and have taken steps to further protect unauthorized access to individual records, including reviewing and revising our information security practices, and bolstering our existing security to reduce the chance of a future incident.

For More 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]. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to help protect against misuse of your information. The response line is available Monday through Friday, 7:00 a.m. to 7:00 p.m. Central Time, excluding holidays. Representatives are available for 90 days.

Sincerely,

Home Care Providers of Texas

– ADDITIONAL PRIVACY SAFEGUARDS INFORMATION –

1. Enrolling in Complimentary twelve (12) -Month Credit Monitoring.

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.



2. 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

3. 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.

4. 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.

5. 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.

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.