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

May 19, 2023

VIA U.S. MAIL

John M. Formella
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301

Re: HealthPlan Services, Inc. – Update to April 28, 2023 Incident Notification

Dear Mr. Formella:

McDonald Hopkins PLC represents HealthPlan Services, Inc. ("HealthPlan Services") located at 4110 George Road, Tampa, Florida. I am writing to provide an update to the notification of an incident on behalf of HPS and impacted third party carriers sent to you on April 28, 2023. HPS has finished notifying potentially affected individuals on behalf of impacted third party carriers. The number of New Hampshire residents has increased from two (2) to three (3) New Hampshire residents. By providing this notice, HealthPlan Services does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

On June 23, 2022 HealthPlan Services detected that some elements within its network had been affected by malware. Upon detecting the incident, HealthPlan Services commenced an immediate and thorough investigation. As part of the investigation, HealthPlan Services worked to identify what personal information, if any, might have been present in the accessed systems.

After a thorough and detailed forensic investigation and comprehensive manual document review, HealthPlan Services determined on February 28, 2023 and March 21, 2023, that resulting from the malware, an unauthorized party accessed and/or acquired certain files or folders from portions of its network containing personal information pertaining to a limited number of individuals. This information included .

HealthPlan Services provided the affected residents with written notification of this incident pursuant to the HIPAA Breach Notification Rule, 45 CFR § 164.404, commencing on April 28, 2023 and ending on May 19, 2023, in substantially the same form as the letter attached hereto.

HealthPlan Services is not aware of any reports of identity fraud or improper use of personal information as a direct result of this incident. However, out of an abundance of caution,

HealthPlan Services wanted to inform your Office (and the affected residents) of the incident. Notified individuals have been provided with best practices to protect their information, including but not limited to complimentary credit monitoring services.

At HealthPlan Services, protecting the privacy of personal information is a top priority. HealthPlan Services is committed to maintaining the privacy of personal information in its possession and has taken precautions to safeguard it. HealthPlan Services continually evaluates and modifies its practices to enhance the security and privacy of the personal information it maintains. Since detecting the incident, HealthPlan Services has reviewed and revised its information security practices, provided additional training to employees, and implemented additional security measures to mitigate the chance of a similar event in the future.

Should you have any questions regarding this notification, please contact me at

Sincerely,

Dominic A. Paluzzi

Encl.

HealthPlan Services, Inc
[redacted]

To Enroll, Please Call:
[redacted]
Or Visit:
[redacted]
Enrollment Code: [XXXXXXXX]

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

April 28, 2023

IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY

<<Variable Header>>

Dear <<First Name>> <<Last Name>>:

We are writing with important information regarding a data security incident that occurred at HealthPlan Services Inc. ("HPS"). HPS provides certain technology-based services for [redacted], which requires access to and storage of certain individual information. The privacy and security of the information we maintain is of the utmost importance to HPS. 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?

HPS detected that some elements within our network had been affected by malware and, as a result, an unauthorized party accessed and/or acquired certain files or folders from portions of our network on June 23, 2022.

What We Are Doing

Upon detecting the incident that same day, HPS commenced an immediate and thorough investigation, contained the network, and alerted law enforcement. As part of our investigation, HPS engaged leading cybersecurity professionals to identify the extent of the activity and what, if any, members' personal information may have been accessed and/or acquired by the unauthorized party. After a thorough and detailed forensic investigation and comprehensive manual document review, on <<February 28, 2023 / March 21, 2023>>, HPS determined that certain personal information may have been acquired in the incident. HPS subsequently moved to notify you about this incident and provide you with information to protect your personal and/or health information. Notification of the incident was not delayed as a result of a law enforcement investigation.

HPS values your privacy and deeply regrets that this incident has occurred. We take the security of your information very seriously and have taken many precautions to safeguard it. We continually evaluate and modify our practices to enhance the security and privacy of your information. Since detecting the incident, we have reviewed and revised our information security practices, provided additional training to employees, and implemented additional security measures to mitigate the chance of a similar event in the future.

What Information Was Involved?

The information potentially involved includes your full name and, <<personal information involved>>.

What You Can Do

To protect you from the potential misuse of your information, we are offering identity theft protection services through IDX, A ZeroFox Company, the data breach recovery services expert. IDX identity protection services include: 24 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised. For more information on identity theft prevention and IDX identity protection services including instructions on how to activate your complimentary 24-month membership, please see the additional information provided in this letter.

This letter also provides other precautionary measures you can take to protect your 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

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have established to respond to questions surrounding the incident at [redacted]. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available Monday through Friday, from 9AM to 9PM Eastern Time, excluding holidays.

Sincerely,

President and CEO
HealthPlan Services, Inc.

OTHER IMPORTANT INFORMATION

Enrolling in Complimentary 24-Month Credit Monitoring

Go to [redacted] and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Please note that the enrollment deadline is July 28, 2023. Note: You must have established credit to use the credit monitoring service. If you need assistance, IDX will be able to assist you.

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 105069
Atlanta, GA 30348
www.equifax.com
1-800-525-6285

Experian
P.O. Box 2002
Allen, TX 75013
www.experian.com
1-888-397-3742

TransUnion
P.O. Box 2000
Chester, PA 19016
www.transunion.com
1-800-680-7289

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.freeze.equifax.com
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 160
Woodlyn, PA 19094
http://www.transunion.com/creditfreeze
1-800-916-8800

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 any credit monitoring service, 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

<<**Protecting Your Health Information**

As a general matter the following practices can help to protect you from medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.

- Review your "explanation of benefits" statement which you receive from your health insurance company. Follow up with your insurance company or the care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential disclosure (June 23, 2022) to current date.

- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or care provider for any items you do not recognize.>>.

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.govadtheft, 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. For more information on preventing and reporting identity theft, you may go to www.ftc.gov/credit.

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.

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.