

Dominic A. Paluzzi
Direct Dial: 248.220.1356
dpaluzzi@mcdonalddhopkins.com

July 21, 2016

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

Re: Virginia Premier Health Plan, Inc. – Incident Notification

2016 JUL 26 P 3:46
OFFICE OF THE ATTORNEY GENERAL

Dear Sir or Madam:

McDonald Hopkins PLC represents Virginia Premier Health Plan, Inc. (VPHP). I write to provide notification concerning an incident that affects the security of personal information of three (3) Maryland residents. VPHP's investigation is ongoing and this notification will be supplemented with any new significant facts or findings subsequent to this submission, if any. By providing this notice, VPHP does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

On July 11, 2016 VPHP discovered that on June 30, 2016, as a result of a complex phishing incident, an unauthorized third party obtained an electronic file containing certain information on current and former employees who received employment earnings in 2015 from VPHP.

Upon learning of the issue, VPHP's incident response team promptly launched an investigation, including reporting the incident to law enforcement. As part of its investigation, VPHP has been working very closely with external cybersecurity professionals who regularly investigate and analyze these types of incidents.

VPHP has devoted considerable time and effort to determine what exact information may have been contained in the affected files and, as such, at risk of disclosure. VPHP has confirmed that the information sent to the unauthorized party included 2015 W-2 information, which included employees' full names, Social Security numbers, home addresses, and earnings for 2015. No spouse or dependent information was sent to the unauthorized party.

To date, VPHP is not aware of any reports of identity fraud as a direct result of this incident. We wanted to make you (and the affected residents) aware of the incident and explain the steps VPHP is taking to help safeguard the residents against identity fraud. VPHP provided the Maryland residents with written notice of this incident commencing on July 21, 2016, in substantially the same form as the letter attached hereto. VPHP is offering the residents a complimentary one-year membership with a credit monitoring and identity theft protection service and is providing dedicated call center support to answer questions. VPHP has advised the residents to remain vigilant in reviewing financial account statements for fraudulent or irregular activity. VPHP has advised the residents about the process for placing a fraud alert on their credit files, placing a security freeze, and obtaining a free credit report. The residents also have been provided with the contact information for your office, the consumer reporting agencies and the Federal Trade Commission.

VPHP takes its obligation to help protect personal information very seriously. VPHP is continually evaluating and modifying its practices to enhance the security and privacy of personal information, including training its workforce on security threats.

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

Sincerely,



Dominic A. Paluzzi

Encl.



600 E. Broad Street
4th Floor, Suite 400
Richmond, VA 23219

***IMPORTANT INFORMATION
PLEASE READ CAREFULLY***

<<mail id>>
<<FirstName>><<LastName>>
<<Address1>>
<<Address2>>
<<City>><<State>><<Zip>>

<<Date>>

Dear <<Name1>>,

The privacy of your personal information is of utmost importance to Virginia Premier Health Plan, Inc. (VPHP). We are writing with important information about a recent incident involving the security of some of our employees' personal information. We wanted to provide you with information regarding the incident and explain the services we are making available to help safeguard you against identity fraud. We also are providing additional steps you can take to help protect your information.

What Happened?

On July 11, 2016 we discovered that on June 30, 2016, as a result of a complex phishing incident, an unauthorized third party obtained an electronic file containing certain information on current and former employees who received employment earnings in 2015 from VPHP.

What Information Was Involved?

We have confirmed that the information sent to the unauthorized party included your 2015 W-2 information, which included your full name, Social Security number, home address, and earnings for 2015. No spouse or dependent information was sent to the unauthorized party.

What We Are Doing.

Upon learning of the issue, our incident response team promptly launched an investigation, including reporting the incident to law enforcement. As part of our investigation, we have been working very closely with external cybersecurity professionals who regularly investigate and analyze these types of incidents. To date, we are not aware of any reports of identity fraud as a direct result of this incident. Out of an abundance of caution, we wanted to make you aware of the incident, explain the services we are making available to help safeguard you against identity fraud, and suggest steps you should take.

What You Can Do.

Enclosed in this letter you will find information on enrolling in a 12-month membership of Experian's ProtectMyID® Alert that we are providing at no cost to you. This robust product, which is being provided directly from one of the three major consumer reporting agencies, helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

Enclosed you will also find other precautionary measures you can take to protect your personal information, including placing a Fraud Alert, placing a Security Freeze, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements for fraudulent or irregular activity on a regular basis.

The information that is likely to be most at risk in this situation is the type of information that may be used to file fraudulent tax returns. As a result, you should contact your tax advisor, if you have one, and let them know that this information may be at risk. You should also file your tax return as quickly as possible, if you have not already done so. (Note: Filing for an extension does not prevent the potential for a fraudulent tax return to be filed.)

If you believe that you are a victim of identity fraud AND it is affecting your federal tax records (or may affect them at some time in the future), such as your attempt to file your federal tax return electronically was rejected or if you received a notice from the IRS indicating someone was otherwise using your Social Security number, it is recommended that you contact your tax advisor, if you have one; file an Identity Theft Affidavit (Form 14039) with the IRS (the form can be downloaded at: <https://www.irs.gov/pub/irs-pdf/f14039.pdf>); call the IRS at (800) 908-4490, ext. 245 to report the situation (the unit office is open Monday through Friday from 7 am to 7 pm); and report the situation to your local police department. Additional information regarding preventing tax related identity theft can be found at <http://www.irs.gov/uac/Identity-Protection>.

As a reminder, always verify the email address and sender of any email you receive requesting confidential or sensitive information. If you have any doubt about a request for confidential information, you should contact the apparent requestor via telephone or in person to confirm the request.

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 protect against misuse of your information. The response line is available Monday through Friday, 9:00 am to 9:00 p.m. Eastern Time.

On behalf of VPHP, please accept our sincere apologies that this incident occurred. Rest assured we have the policies and procedures in place to protect your personal information. However, we continually evaluate and modify our practices to enhance the security and privacy of your information, including training our workforce on security threats. Please know that we are devoting considerable resources so that our employees are fully informed and are provided with some protection as a result of this unfortunate incident.

Sincerely,

[REDACTED]

Carl Gattuso
Interim Chief Executive Officer
Virginia Premier Health Plan, Inc.

– ADDITIONAL PRIVACY SAFEGUARDS INFORMATION –

1. Enrolling in Complimentary 12-Month Credit Monitoring.

Protecting your personal information is important to Virginia Premier Health Plan, Inc. In response to this security incident and as a precautionary measure, we have arranged for you to enroll in Experian's® ProtectMyID® Alert for a one year period at no cost to you. This protection is provided by Experian, one of the three major nationwide credit reporting companies.

Activate Experian's® ProtectMyID Now in Three Easy Steps:

1. ENSURE that you enroll by **October 21, 2016**.
2. VISIT the ProtectMyID Web Site to enroll: www.protectmyid.com/redeem
3. PROVIDE your 9-character Activation Code: <<XXXXXXXXXX>>

If you have questions or need an alternative to enrolling online, please call [REDACTED] and provide Engagement # [REDACTED]

Additional Details Regarding Your 12-Month ProtectMyID Membership:

A credit card is not required for enrollment.

Once your ProtectMyID membership is activated, you will receive the following features:

- **Free copy of your Experian credit report**
- **Surveillance Alerts for:**
 - **Daily Bureau Credit Monitoring:** Alerts of key changes & suspicious activity found on your Experian, Equifax® and TransUnion® credit reports.
- **Identity Theft Resolution & ProtectMyID ExtendCARE:** Toll-free access to US-based customer care and a dedicated Identify Theft Resolution agent who will walk you through the process of fraud resolution from start to finish for seamless service. They will investigate each incident; help with contacting credit grantors to dispute charges and close accounts including credit, debit and medical insurance cards; assist with freezing credit files; contact government agencies.
 - It is recognized that identity theft can happen months and even years after an incident. To offer added protection, you will receive ExtendCARE™, which provides you with the same high-level of Fraud Resolution support even after your ProtectMyID membership has expired.
- **\$1 Million Identity Theft Insurance:** Immediately covers certain costs including lost wages, private investigator fees, and unauthorized electronic fund transfers. (Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of AIG. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.)

Once your enrollment in ProtectMyID is complete, you should carefully review your credit report for inaccurate or suspicious items. If you have any questions about ProtectMyID, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at [REDACTED]

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
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 19022
www.transunion.com
1-800-680-7289

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. 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

PO Box 105788
Atlanta, GA 30348
<https://www.freeze.equifax.com>
1-800-685-1111

Experian Security Freeze

PO Box 9554
Allen, TX 75013
<http://experian.com/freeze>
1-888-397-3742

TransUnion Security Freeze

P.O. Box 2000
Chester, PA 19022
<http://www.transunion.com/securityfreeze>
1-800-680-7289

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.

In addition to the FTC, the Maryland Office of the Attorney General can also be contacted to obtain information on the steps you can take to avoid identity theft:

Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023
www.oag.state.md.us

6. Reporting Identity Fraud to the IRS.

If you believe that you are a victim of identity fraud AND it is affecting your federal tax records (or may affect them at some time in the future), such as your attempt to file your federal tax returns electronically was rejected or if you received a notice from the IRS indicating someone was otherwise using your Social Security number, it is recommended that you do the following:

- Contact your tax preparer, if you have one.
- File an Identity Theft Affidavit (Form 14039) with the IRS. The form can be downloaded at: <http://www.irs.gov/pub/irs-pdf/f14039.pdf>

- Call the IRS at (800) 908-4490, ext 245 to report the situation. The unit office is open Monday through Friday from 7 am to 7 pm.
- Report the situation to your local police department.

Additional information regarding preventing tax related identity theft can be found at <http://www.irs.gov/uac/Identity-Protection>.

7. Reporting Identity Fraud to the Social Security Administration.

If you believe that you are a victim of identity fraud AND it is affecting your Social Security account or records, you may contact the Social Security Administration at 1-800-772-1213 or visit https://secure.ssa.gov/acu/IPS_INTR/blockaccess. You also may review earnings posted to your record on your Social Security Statement on www.socialsecurity.gov/myaccount.

- The Social Security Administration has published Identity Theft and Your Social Security Number at: <https://www.ssa.gov/pubs/EN-05-10064.pdf>.