

**Dominic A. Paluzzi**  
Direct Dial: 248.220.1356  
dpaluzzi@mcdonaldhopkins.com

April 20, 2016

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

2016 APR 20 PM 4:59  
7761

**Re: Anthelio Healthcare Solutions Inc. – Incident Notification**

Dear Sir or Madam:

McDonald Hopkins PLC represents Anthelio Healthcare Solutions Inc. (“Anthelio”). I write to provide notification concerning an incident that may affect the security of personal information of twenty (20) Maryland residents. Anthelio’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, Anthelio does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

On April 4, 2016 Anthelio discovered that on February 25, 2016, as a result of a phishing incident, an unauthorized third party may have received an electronic file containing certain information on current and former employees who received employment earnings in 2015 from Anthelio. Upon learning of the issue, Anthelio’s incident response team promptly launched an investigation, including reporting the incident to law enforcement. As part of its investigation, Anthelio has been working very closely with external cybersecurity professionals who regularly investigate and analyze these types of incidents.

Anthelio 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. Anthelio has confirmed that the electronic file contained 2015 W-2 information, which included full names, Social Security numbers, home addresses, and earnings.

We wanted to make you (and the affected residents) aware of the incident and explain the steps Anthelio is taking to help safeguard the residents against identity fraud. Anthelio will be providing the Maryland residents with written notice of this incident commencing on April 20, 2016, in substantially the same form as the letter attached hereto. Anthelio is offering the residents a complimentary membership with a credit monitoring and identity theft protection service and is providing dedicated call center support to answer questions. Anthelio will advise the residents to remain vigilant in reviewing financial account statements for fraudulent or irregular activity. Anthelio will advise 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 will be provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

Anthelio takes its obligation to help protect personal information very seriously. Anthelio is continually evaluating and modifying its practices to enhance the security and privacy of personal information.

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

Sincerely,



Dominic A. Paluzzi

Encl.



A higher aim. A newer standard.

<<Date>>

**IMPORTANT INFORMATION  
PLEASE READ CAREFULLY**



Dear [Redacted]

The privacy of your personal information is of utmost importance to Anthelio Healthcare Solutions Inc. We are writing with important follow-up information about a recent incident involving the security of our employees' personal information. We wanted to provide you with additional 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 April 4, 2016 we discovered that on February 25, 2016, as a result of a phishing incident, an unauthorized third party may have received an electronic file containing certain information on current and former employees who received employment earnings in 2015 from Anthelio.

*What Information Was Involved?*

We have confirmed that the electronic file contained your 2015 W-2 information, which included your full name, Social Security number, home address, and earnings.

*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. While we cannot make a direct link to this incident, we are aware that some employees have recently experienced tax fraud issues. Thus, 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 you will find information on enrolling in a 1-year membership in AllClear PRO TBO from AllClear ID, which is a three-bureau option credit monitoring and identity theft resolution service that we are providing at no cost to you, along with 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.

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 EDT); and/or 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>.

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 [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 Saturday, 9:00 am to 9:00 p.m. Eastern Time.

On behalf of Anthelio, please accept our sincere apologies that this incident occurred. We continually evaluate and modify our practices to enhance the security and privacy of your information. Please know that we are devoting considerable resources to ensure our employees are fully informed and protected as a result of this unfortunate incident.

Sincerely,

[REDACTED]

- ADDITIONAL PRIVACY SAFEGUARDS INFORMATION -

**1. Enrolling in Complimentary 1-Year Credit Monitoring and Identity Theft Restoration Services.**

Protecting your personal information is important to Anthelio Healthcare Solutions, Inc. As an added precaution, we have arranged to have AllClear ID protect your identity for one year at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next year.

**AllClear SECURE:** The team at AllClear ID is ready and standing by if you need identity repair assistance. This service is automatically available to you with no enrollment required. If a problem arises, simply call [REDACTED] and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

**AllClear PRO TBO:** This service offers additional layers of protection including credit monitoring and a \$1 million identity theft insurance policy. To use the PRO TBO service, you will need to provide your personal information to AllClear ID. You may sign up online at [REDACTED] or by phone by calling [REDACTED] using the following redemption code: [REDACTED]

Please note: Additional steps may be required by you in order to activate your phone alerts and monitoring options.

**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

Include applicable fee (if any). Call or visit each of the credit reporting company websites listed above for information on fees for Security Freeze services. Forms of payment are check, money order, or credit card (American Express, Discover, MasterCard and Visa), or a copy of a valid identity theft report, or other valid report from a law enforcement agency to show you are a victim of identity theft and are eligible for free Security Freeze services.

#### **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](http://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](http://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](http://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: <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.
- 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/aku/IPS\\_INTR/blockaccess](https://secure.ssa.gov/aku/IPS_INTR/blockaccess). You also may review earnings posted to your record on your Social Security Statement on [www.socialsecurity.gov/myaccount](http://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>.