McDermott
Will & Emery

Boston Brussels Chicago Düsseldorf Frankfurt Houston London Los Angeles Miami
Milan Munich New York Orange County Paris Rome Seoul Silicon Valley Washington, D.C.
Strategic alliance with MWE China Law Offices (Shanghai)

[redacted]

March 12, 2015

VIA EMAIL (attorneygeneral@doj.nh.gov)

New Hampshire Attorney General Joseph Foster
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Anthem, Inc. Data Breach

Dear Attorney General Foster:

Pursuant to New Hampshire's Right to Privacy Act, §359-C:1, and our previous communication to you dated February 27, 2015, we write to update you with further information that McDermott Will & Emery LLP ("McDermott") has learned about the Anthem, Inc. ("Anthem") data breach. As stated in our February 27, 2015 letter, the health insurance plan that McDermott provides to its employees is the McDermott BlueCross BlueShield medical plan ("the Plan"). The Plan is administered by BlueCross BlueShield of Illinois ("BCBSIL"), and not by Anthem. However, we understand from BCBSIL that Anthem plays a role in processing claims for the McDermott Plan participants who have received medical care and services in states where Anthem operates. Anthem is a service provider to BCBSIL.

Since first learning of the Anthem data breach, we have been in direct communication with BCBSIL. BCBSIL has now informed us of the specific Plan members who were impacted by the data breach. Based on the information we have received from BCBSIL as of the date of this letter, there are 11 residents of your state that were impacted by the data breach. The information affected includes: name (first and last), date of birth, health plan identification number (***not*** Social Security Number), mailing address, and email address (if BCBSIL had it on file).

We are sending out notifications to our affected Plan members in your state this week, and I enclose a template copy of the notification with this letter. If McDermott subsequently learns from BCBSIL that any additional McDermott Plan participants who are residents of your state have been impacted, we will notify them promptly.

We understand that Anthem may have previously notified you of this incident, and we also understand that both Anthem and BCBSIL are notifying our impacted Plan participants directly. Because McDermott is the owner of information about our employees that may have

[redacted]

been compromised by this cyber-attack, we are writing separately to notify you of the incident and meet any obligations we may have under state law.

If you have any questions please do not hesitate to contact me.

Sincerely,

Enclosure

DM_US 59357629-1.T10655.0010

Template Notification Letter Enclosure

Boston Brussels Chicago Düsseldorf Frankfurt Houston London Los Angeles Miami
Milan Munich New York Orange County Paris Rome Seoul Silicon Valley Washington, D.C.
Strategic alliance with MWE China Law Offices (Shanghai)

Linda M. Doyle
Attorney at Law
ldoyle@mwe.com
+1 312 984 6905

March __, 2015

MWE Plan Participant
Address 1
Address 2
City, State Zip

Re: Anthem Data Breach – Notice Concerning Disclosure of Your Personal Information

Dear Name:

We write to follow up on the information provided in our letter to you dated March 2, 2015 regarding the Anthem, Inc. ("Anthem") data breach[1]. As you may know, Anthem is the largest of the Blue Cross and Blue Shield Plans, and recently announced it was the target of a sophisticated cyber-attack resulting in a data breach. The McDermott Will & Emery Group Health Plan's medical plan ("Plan") is administered by Blue Cross Blue Shield of Illinois ("BCBSIL") and not by Anthem. Anthem, however, assists BCBSIL in processing claims for the Plan and, as a result, receives participants' personal information. Since learning of the incident, we have been in regular contact with BCBSIL to understand the extent to which our Plan participants' information is impacted by this incident.

Your Personal Information Affected By The Anthem Breach

BCBSIL has now informed us that your personal information is affected. BCBSIL identified you as a [current or former] Plan member whose name (first and last), date of birth [if applicable], health plan identification number (***not*** Social Security Number), mailing address, and email address (if BCBSIL had it on file) were exposed in the data breach.

This information is based on what BCBSIL has reported to us as of the date of this letter. If we receive any further information regarding the disclosure of your personal information, we will inform you promptly. Anthem has reported that there is no evidence that any medical information (such as claims, test results, or diagnostic codes) or payment card information was compromised in the breach.

You may receive similar notices from BCBSIL or Anthem regarding the breach that are likely to be less specific about what personal information of yours was affected. We wanted to alert you

[1] Note regarding template letter: McDermott sent an initial communication to all its Plan members to inform them of the Anthem data breach, but at the time of that communication, we did not know which (if any) Plan members were actually impacted.

separately so that we can be sure you are informed as to the exact personal information that was compromised in the Anthem breach as reported to us by BCBSIL.

Next Steps and Precautions

We are providing detailed information regarding steps you can take in response to the Anthem data breach at the end of this letter. Although you have already received this information, we provide it again here for ease of reference.

Finally, as we have stated previously, please be cautious of any ***emails*** purporting to be from Anthem or from BCBSIL regarding this incident. We understand that Anthem and BCBSIL will be communicating with affected individuals by **first-class mail**. To contact Anthem, please use its website, www.AnthemFacts.com, or call its toll-free number, 1-877-263-7995. Please see the end of this package for additional information on detecting and preventing email hoaxes related to the Anthem data breach.

The Firm takes its obligations to protect the personal information of its attorneys and staff (current and former) seriously. If you have any questions for the Firm, please contact the McDermott Benefits Team at HumanResourcesBenefits@mwe.com or (312) 984-7575.

Sincerely,

Linda M. Doyle

I. Identity Protection Services Through Anthem

Anthem's dedicated website explains the identity protection services that it is offering to affected participants. Anthem represents that it is offering two identity protection services through its vendor AllClearID, which you can learn more about by visiting the Anthem website or calling Anthem using the information below. The first service, available to you for a 24 month coverage period and for free, is described as a preventive credit monitoring service. This service requires you to register and provide certain personal information (including your Social Security Number) to activate the service. The second service is described as an identity repair assistance service, which is automatically available to you for 24 months with no enrollment required. If a problem arises, Anthem's website indicates that you would contact AllClearID and an investigator will work to recover financial losses, restore your credit, and work to return your identity to its proper condition.

- **Anthem's dedicated website: www.AnthemFacts.com**
- **Anthem's toll-free number: 1-877-263-7995**

II. Other Identity Protection Services

Obtaining Your Credit Report; Fraud Alerts; Credit Freezes

Credit Reports: We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax, P.O. Box105139, Atlanta, Georgia 30374-0241, 1-800-685-1111, www.equifax.com
Experian, P.O. Box 2002, Allen, TX 75013, 1-888-397-3742, www.experian.com
TransUnion, P.O. Box 6790, Fullerton, CA 92834-6790, 1-800-916-8800, www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

Fraud Alerts: There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90

days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three national credit reporting agencies listed below.

Equifax: 1-800-525-6285, www.equifax.com
Experian: 1-888-397-3742, www.experian.com
TransUnion: 1-800-680-7289, www.transunion.com

Credit or "Security" Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit reporting company. *Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.*

Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified above (TransUnion, Experian and Equifax) to find out more information.

For example, here are the **Security Freeze Instructions for Massachusetts Residents**:

If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift or remove a security freeze. Otherwise, a credit reporting agency may charge you up to $5.00 each to place, temporarily lift, or permanently remove a security freeze. In order to request a security freeze, you will need to provide the following information:

1. *Your full name (including middle initial as well as Jr., Sr., II, III, etc.);*
2. *Social Security Number;*
3. *Date of birth;*
4. *If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;*
5. *Proof of current address such as a current utility bill or telephone bill;*
6. *A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)*

7. *If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;*
8. *If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.*

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) ***and*** *the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.*

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) ***and*** *the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.*

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.

Other Resources

We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding identity theft.

Federal Trade Commission, Consumer Response Center
600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338),
www.ftc.gov/idtheft

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

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

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

> **North Carolina Attorney General's Office**, Consumer Protection Division
> 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov

III. Warnings About Email and Phone Scams

Please be aware that scams involving either emails that say they are from Anthem with attachments or web links (phishing) or fake telephone calls have surfaced.

Here are some critical scam/hoax email tips to bear in mind:

- DO NOT click on any links in an email that look like they are coming from Anthem.
- DO NOT reply to any Anthem email or reach out to the senders in any way.
- DO NOT supply any information on the website that may open if you have clicked on link in an Anthem-related email.
- DO NOT open any attachments that arrive with Anthem email.
- DO NOT provide any of your personal information over the phone if you *receive* a call from someone from Anthem.
- REPORT to security@mwe.com if you have received any of these emails or phone calls.
- DO check your credit card and bank statements for any suspicious charges or entries.
- DO check your credit reports periodically.