NUANCE COMMUNICATIONS, INC. ONE WAYSIDE ROAD
BURLINGTON, MA 01803

[redacted]

NUANCE

March 20, 2015

VIA EMAIL to attorneygeneral@doj.nh.gov

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

RE: Anthem Data Breach

Dear Attorney General Foster:

Pursuant to New Hampshire General Statutes, and Right to Privacy Act, we write to inform you that Anthem, Inc. ("Anthem") is a downstream subcontractor to one of our self-funded group health plans ("Plan"). Our Plan is administered by Blue Cross Blue Shield of Massachusetts ("BCBSMA"), and not by Anthem. However, we understand from BCBSMA that Anthem plays a role in processing claims for our Plan participants who have received medical care and service in certain circumstances, such as when a participant receives medical care in an Anthem state.

As you are aware, Anthem was the victim of a cyber-attack, commencing on or about December 10, 2014 ("Incident'). We understand from media reports that Anthem initially discovered the Incident on or about January 27, 2015. We were first informed of the Incident by our insurance broker on February 5, 2015, but there was no information whether and to what extent any of our Plan participants were impacted. We have been in communication with BCBSMA representatives, who since informed us on March 2, 2015, that 1260 members of our Plan were impacted, 152 of whom reside in your state.

BCBSMA states the personal information accessed in the Anthem data breach included: first name, last name, subscriber ID, gender, city, state, zip code, and date of birth. It further states that only a small fraction of its affected members had their social security numbers accessed. According to BCBSMA, no credit card, medical, or financial information was accessed for any of its members. We are not aware of any fraud that has occurred as a result of this incident.

We are working with BCBSMA to identify the precise data elements impacted for each affected participant. We also are working with BCBSMA to ensure that they send notices to each impacted Plan participant. In the meantime, we have emailed our participants with the attached notification more generally, to alert them to this issue in advance of the communication from BCBSMA.

If you have any questions for us, please contact me.

Sincerely,

GRETCHEN S. HERAULT
Deputy Chief Privacy Officer

NUANCE COMMUNICATIONS, INC.

[redacted]

Credit Reports

Periodically check your credit report from each of the three major credit bureaus (Equifax, Experian and TransUnion) for fraudulent activity. You can obtain a copy of each report free once a year from each of the three credit bureaus. You may be entitled to additional free reports if you've been a victim of identity theft. If you find inaccuracies on your report, dispute them immediately.

Personal Identity Information

- Keep all identification and financial documents in a safe and private place.
- Provide personal information only when you know how it will be used, you are certain it won't be shared, and you've initiated contact and know who you're dealing with.
- Make all passwords hard to guess by using a complex combination of numbers and upper and lower case letters.
- Request a vacation hold if you can't pick up your mail and deposit outgoing mail in post office collection boxes or at your local post office.
- Be aware of your workplace's security procedures and keep your purse or wallet in a safe place.
- Do not carry your Social Security card or have it or your driver license number printed on your checks. Share this information only when necessary and to those you trust.

Credit Card, ATM, Debit Cards, Checking Accounts, and Medical ID Cards

- Photocopy both sides of your credit cards so you have all the account numbers, expiration dates and phone numbers, and keep the copies in a safe place. Carry only those cards you really need and cancel unused accounts.
- Shred all statements and pre-approved credit card offers with a crosscut shredder.
- Be aware of people behind you at the ATM, or anywhere else you swipe your card. If you give your credit or debit card to someone for a transaction, watch them swipe it and inspect the receipt for accuracy.
- Know your billing cycles & contact your creditors if your statements don't arrive on time.
- Know where your checkbook is at all times. When you write a check, be sure to print firmly and use indelible ink. Check your account statement for fraudulent activity.
- Examine your transactions online or on your statements each month.
- Read the Explanations of Benefits (EOBs) you receive from your Health Plan. Make sure the health care claims to your insurer match the items and services provided. If there is a discrepancy, contact your insurer immediately.

Computer

- Update your virus protection software periodically, and after every new virus alert is announced. Also, use a firewall program to prevent your computer from being accessible to hackers.
- Do not download files or open hyperlinks sent from people you don't know.
- Use a secure browser to guard the security of your online transactions. Enter personal and financial information only when there is a "lock" icon on the browser's status bar and look for the URL to read "https" versus "http".
- If you must store personal and financial information on your laptop, use a strong password—one that is a hard-to-guess combination of upper and lower case letters and numbers, don't use an automatic log-in feature, and always log off when you're finished.

Recovery Guide

If you are a victim of identity theft, understand that minimizing damage will take patience and a systematic approach. However, the sooner and more aggressively you deal with the problem, the faster you will see results.

To start, commit yourself to becoming and remaining organized. Since you will be communicating with a lot of people and have many tasks to complete. Keep copies of all letters, file paperwork promptly, and store everything in a safe and accessible place.

Creditors and Financial Institutions

- If accounts have been used or opened illegally, contact your creditors immediately. For any compromised account, you should get a new account number and card. You may need to provide the creditor with a police report or the Federal Trade Commission's *Identity Theft Victim's Complaint and Affidavit*. Monitor all future account statements carefully for evidence of new fraud.
- If a collection agency attempts to collect on a fraudulent account, explain (in writing) that you are a victim of identity theft and not responsible for the debt. Ask that they confirm in writing that you do not owe the balance and that the account has been closed.
- For checking account fraud, contact your financial institution to place stop payments on any outstanding checks that you did not write. Close current checking and savings accounts and obtain new account numbers and passwords.

Legal and Government Agencies

- Report the crime and file a police report. Request a copy of the report and keep the phone number of your investigator handy. A complaint can also be filed with the Federal Trade Commission, although they do not assist with individual cases.
- Notify the US Postal Inspection Service if your mail was stolen or your address was used fraudulently.

Credit Reporting Bureaus

- Check your credit reports from all three bureaus, Equifax, Experian, and TransUnion. Dispute any fraudulent items—this can be done by submitting a form online or mailing a letter to the credit bureaus.
- Even if the fraudulent information hasn't yet appeared on your reports, be proactive and report the crime to credit bureaus now. It is a good idea to have a fraud alert placed on your credit reports. When someone applies for credit under your name, the creditor must verify that the person applying is you. The initial fraud alert only lasts 90 days. However, if you file a police report, you can extend the alert to 7 years.

Helpful Resources

Equifax
To order a credit report call: (800) 685-1111
To report fraud call: (888) 766-0008
http://www.equifax.com/

Experian
To order a credit report and report a fraud call: (888) 397-3742
http://www.experian.com/

TransUnion
To order a credit report call: (800) 888-4213
To report fraud call: (800) 680-7289
http://www.transunion.com/

Annual Credit Report Request Service
(877) 322-8228
https://www.annualcreditreport.com/index.action

U.S. Federal Trade Commission (FTC)
(877) 438-4338
http://www.ftc.gov/

March 20, 2015

Name
Address
Address

Dear Nuance Medical Plan Participant:

On January 29, 2015, Anthem, Inc. (Anthem) discovered that it was the target of what it has determined was a very sophisticated external cyber-attack. The Group Medical Benefits portion of the Nuance Communications, Inc. Health and Welfare Life Insurance, Long-Term Disability & Travel Accident Plan (the Plan) is administered by Blue Cross Blue Shield of Massachusetts (BCBSMA). BCBSMA and Anthem are part of a series of independent but networked Blue Cross Blue Shield companies across the country that help facilitate the payment for medical services. When a plan participant seeks medical services outside of Massachusetts, the local BCBS affiliate (such as Anthem) will process the claim and store your medical data.

According to Anthem, you received care in one of the states that Anthem covers, which includes California, Colorado, Connecticut, Georgia, Indiana, Kentucky, Maine, Missouri, Nevada, New Hampshire, New York, Ohio, Virginia and Wisconsin. As a result, your information was accessed during the breach.

What Personal Information was involved in the incident?
Anthem states that their current investigation indicates there was unauthorized access to the following data: *name, date of birth, gender, health plan member ID, address, phone number, email address and employment information*. At this time, they have no reason to believe that social security numbers, credit/debit card or banking information was compromised, nor is there evidence that medical information, such as claims, test results, or diagnosis/procedure codes, was obtained.

What will happen next?

- During the week of March 2, 2015, BCBSMA sent letters to members confirming that they were impacted. Please call BCBSMA at 1-888-404-9846 if you did not receive a letter.
- You will also receive a notification directly from Anthem regarding this incident which will provide you with additional information about a program that Anthem is offering that includes two years of free credit monitoring and identity protection services. You can pro-actively learn more and sign up immediately by visiting www.anthemfacts.com.
- In addition to signing up for credit monitoring and identify protection services, you should carefully review any Explanations of Benefits (EOBs) that you receive from BCBSMA and other insurance companies. Make sure the health care claims reflected in these EOBs accurately reflect the items and services that you received. Look for the name of the provider, the date of service and the service provided. If there is a discrepancy, immediately contact BCBSMA member services at 1-800-588-5508 to report the problem.
- You may call into the BCBSMA member services (1-800-588-5508) and request a new subscriber ID number.

Phone and Email scams

You should be aware of Phone and Email scam campaigns targeting current and former Anthem members. Anthem is not calling members regarding the cyber-attack and is not asking for credit card information or Social Security numbers over the phone. There have been reports of email scams designed to capture personal information (known as “phishing”), that appear as if they are from Anthem and the emails include a “click here” link for credit monitoring. These emails are NOT from Anthem.

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

- DO check your credit card and bank statements for any suspicious charges or entries.
- DO check your credit reports periodically.
- DO NOT reply to the 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 a link in the email.
- DO NOT open any attachments that arrive with email.

For more guidance on recognizing scam emails, please visit the FTC Website:
http://www.consumer.ftc.gov/articles/0003-phishing

Questions
Visit Anthem’s website dedicated to the incident– www.AnthemFacts.com (http://www.AnthemFacts.com). You may also call Anthem’s dedicated toll-free number, 1-877-263-7995, to ask questions.

ADDITIONAL INFORMATION ABOUT IDENTITY THEFT PREVENTION

Review Your Credit Reports
You should 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 for any sign of fraud such as accounts or creditor inquiries that you did not initiate or do not recognize, debts that you cannot explain, medical debt collection notices from health care providers or a home address or 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
You should also consider placing a fraud alert to put your creditors and potential creditors on notice that you may be a victim of fraud. 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.

What if You Find Evidence of Identity Theft or Other Suspicious Activity?
You should promptly report any suspicious activity or suspected identity theft 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 regulatory authorities 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

March 20, 2015

NAME
ADDRESS
ADDRESS

Dear NTS Medical Plan Participant:

On January 29, 2015, Anthem, Inc. (Anthem) discovered that it was the target of what it has determined was a very sophisticated external cyber-attack. The Group Medical Benefits portion of the Nuance Communications, Inc. Health and Welfare Life Insurance, Long-Term Disability & Travel Accident Plan (the Plan) is administered by Blue Cross Blue Shield of Massachusetts (BCBSMA). BCBSMA and Anthem are part of a series of independent but networked Blue Cross Blue Shield companies across the country that help facilitate the payment for medical services. When a plan participant seeks medical services outside of Massachusetts, the local BCBS affiliate (such as Anthem) will process the claim and store your medical data.

According to Anthem, you received care in one of the states that Anthem covers, which includes California, Colorado, Connecticut, Georgia, Indiana, Kentucky, Maine, Missouri, Nevada, New Hampshire, New York, Ohio, Virginia and Wisconsin. As a result, your information was accessed during the breach.

What Personal Information was involved in the incident?
Anthem states that their current investigation indicates there was unauthorized access to the following data: *name, date of birth, gender, health plan member ID, address, phone number, email address and employment information*. At this time, they have no reason to believe that social security numbers, credit/debit card or banking information was compromised, nor is there evidence that medical information, such as claims, test results, or diagnosis/procedure codes, was obtained.

What will happen next?

- During the week of March 2, 2015, BCBSMA sent letters to members confirming that they were impacted. Please call BCBSMA at 1-888-404-9846 if you did not receive a letter.
- You will also receive a notification directly from Anthem regarding this incident which will provide you with additional information about a program that Anthem is offering that includes two years of free credit monitoring and identity protection services. You can pro-actively learn more and sign up immediately by visiting www.anthemfacts.com.
- In addition to signing up for credit monitoring and identify protection services, you should carefully review any Explanations of Benefits (EOBs) that you receive from BCBSMA and other insurance companies. Make sure the health care claims reflected in these EOBs accurately reflect the items and services that you received. Look for the name of the provider, the date of service and the service provided. If there is a discrepancy, immediately contact BCBSMA member services at 1-800-588-5508 to report the problem.
- You may call into the BCBSMA member services (1-800-588-5508) and request a new subscriber ID number.

Phone and Email scams

You should be aware of Phone and Email scam campaigns targeting current and former Anthem members. Anthem is not calling members regarding the cyber-attack and is not asking for credit card information or Social Security numbers over the phone. There have been reports of email scams designed to capture personal information (known as “phishing”), that appear as if they are from Anthem and the emails include a “click here” link for credit monitoring. These emails are NOT from Anthem.

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

- DO check your credit card and bank statements for any suspicious charges or entries.
- DO check your credit reports periodically.
- DO NOT reply to the 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 a link in the email.
- DO NOT open any attachments that arrive with email.

For more guidance on recognizing scam emails, please visit the FTC Website:
http://www.consumer.ftc.gov/articles/0003-phishing

Questions
Visit Anthem’s website dedicated to the incident– www.AnthemFacts.com (http://www.AnthemFacts.com). You may also call Anthem’s dedicated toll-free number, 1-877-263-7995, to ask questions. Additionally, NTS has posted information about Identity Theft Prevention on the Enrich intranet website.

NUANCE

March 20, 2015

Name
Address
Address

Dear Nuance Medical Plan Participant:

On January 29, 2015, Anthem, Inc. (Anthem) discovered that it was the target of what it has determined was a very sophisticated external cyber-attack. The Group Medical Benefits portion of the Nuance Communications, Inc. Health and Welfare Life Insurance, Long-Term Disability & Travel Accident Plan (the Plan) is administered by Blue Cross Blue Shield of Massachusetts (BCBSMA). BCBSMA and Anthem are part of a series of independent but networked Blue Cross Blue Shield companies across the country that help facilitate the payment for medical services. When a plan participant seeks medical services outside of Massachusetts, the local BCBS affiliate (such as Anthem) will process the claim and store your medical data.

According to Anthem, you received care in one of the states that Anthem covers, which includes California, Colorado, Connecticut, Georgia, Indiana, Kentucky, Maine, Missouri, Nevada, New Hampshire, New York, Ohio, Virginia and Wisconsin. As a result, your information was accessed during the breach.

What Personal Information was involved in the incident?
Anthem states that their current investigation indicates there was unauthorized access to the following data: *name, date of birth, gender, health plan member ID, address, phone number, email address and employment information*. At this time, they have no reason to believe that social security numbers, credit/debit card or banking information was compromised, nor is there evidence that medical information, such as claims, test results, or diagnosis/procedure codes, was obtained.

What will happen next?

- During the week of March 2, 2015, BCBSMA sent letters to members confirming that they were impacted. Please call BCBSMA at 1-888-404-9846 if you did not receive a letter.
- You will also receive a notification directly from Anthem regarding this incident which will provide you with additional information about a program that Anthem is offering that includes two years of free credit monitoring and identity protection services. You can pro-actively learn more and sign up immediately by visiting www.anthemfacts.com.
- In addition to signing up for credit monitoring and identify protection services, you should carefully review any Explanations of Benefits (EOBs) that you receive from BCBSMA and other insurance companies. Make sure the health care claims reflected in these EOBs accurately reflect the items and services that you received. Look for the name of the provider, the date of service and the service provided. If there is a discrepancy, immediately contact BCBSMA member services at 1-800-588-5508 to report the problem.
- You may call into the BCBSMA member services (1-800-588-5508) and request a new subscriber ID number.

Phone and Email scams

You should be aware of Phone and Email scam campaigns targeting current and former Anthem members. Anthem is not calling members regarding the cyber-attack and is not asking for credit card information or Social Security numbers over the phone. There have been reports of email scams designed to capture personal information (known as "phishing"), that appear as if they are from Anthem and the emails include a "click here" link for credit monitoring. These emails are NOT from Anthem.

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

- DO check your credit card and bank statements for any suspicious charges or entries.
- DO check your credit reports periodically.
- DO NOT reply to the 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 a link in the email.
- DO NOT open any attachments that arrive with email.

For more guidance on recognizing scam emails, please visit the FTC Website:
http://www.consumer.ftc.gov/articles/0003-phishing

Questions
Visit Anthem's website dedicated to the incident– www.AnthemFacts.com (http://www.AnthemFacts.com). You may also call Anthem's dedicated toll-free number, 1-877-263-7995, to ask questions. Additionally, Nuance has posted information about Identity Theft Prevention on the Financial Wellness section of the Nuance Healthy Living page found on The Voice.

Identity Theft Solutions

Your wallet is missing. Thousands of dollars have been charged to your credit cards, your checking account is empty, and loans you never took out appear on your credit report. What happened? You've been a victim of identity theft—an increasingly common and inventive crime.

Identity theft occurs when someone uses your personal information to commit fraud or other crimes. It may also involve computer, mail, wire, and financial institution fraud.

Fortunately, there are preventative measures you can take to substantially reduce the chance of identity theft from occurring, as well as steps to recover from any damage if you are a victim.

Common Practices

How Your Information Is Obtained

Thieves use a variety of illegal techniques to obtain identity information. They may:

- Take mail from a mailbox, or divert mail to another location by filling out a change of address form
- Go through trash to find identification and financial documents
- Access credit reports by posing as landlords or employers
- Hack into personal computers
- Pose as legitimate companies or government agencies to request personal information via e-mail (called *phishing*) or text message (called *smishing*)
- Steal hard copy or electronic files from your workplace
- Stand close to you at the ATM to learn your Personal Identification Number (PIN)
- Attach a skimmer to an ATM to capture the card number and PIN

How Your Information May be Used

Once identity thieves have your personal information, they may use it to:

- Charge on existing credit accounts or open new credit accounts in your name
- Use existing or open new checking accounts in your name and write bad checks
- Establish phone or wireless service in your name
- Use your debit cards or counterfeit checks to drain your checking account
- Take out loans to buy cars and other big ticket items
- Use your identity to obtain medical services

Preventing Identity Theft

There are many ways to protect your private information from fraud. Some tasks take a bit of effort, be aware that cleaning up the mess identity thieves leave behind is far more difficult and time-consuming.