BlueCross BlueShield of Tennessee

1 Cameron Hill Circle
Chattanooga, Tennessee 37402

www.bcbst.com

Bill Young
Senior Vice President of
Risk Management and
General Counsel

[redacted]

March 31, 2010

VIA FEDERAL EXPRESS

Attorney General Michael A. Delaney
Office of Attorney General
33 Capitol Street
Concord, New Hampshire 03301

Dear General Delaney:

I am General Counsel to BlueCross BlueShield of Tennessee, Inc. ("BlueCross"), and I am writing to notify you of a theft of data from a data closet located at a leased facility used by BlueCross in Chattanooga, Tennessee. Specifically, on the evening of Friday, October 2, 2009, unknown persons entered a data closet and removed 57 hard drives. BlueCross employees discovered the theft the following Monday, October 5, 2009, and immediately reported it to law enforcement. The theft of the drives involves some of our members who reside in the State of New Hampshire, and we have already been notifying these members as soon as identified, on a rolling basis. We began notifying our members of the theft on December 7, 2009. Thus far we believe the breach may have impacted 724 of our members who are New Hampshire residents. This number may increase as we finalize processing reviewed data.

Upon learning of the data theft on Monday, October 5, 2009, BlueCross immediately began the process of restoring its back-up tapes of the hard drives at issue. On October 7, 2009, BlueCross reported the theft to the Secretary of the United States Department of Health and Human Services ("HHS").

BlueCross has also notified and met with Tennessee's Attorney General, Robert Cooper, and his staff. We have also provided periodic status updates regarding our investigation and efforts to review the large amount of data to the Office of Civil Rights of HHS which enforces the HIPAA laws. HHS is currently conducting a compliance review of BlueCross.

The stolen hard drives contained recorded telephone calls from providers and members to BlueCross's customer service representatives relating to eligibility and coordination of care. The drives also contained video "screen shots" of the BlueCross customer service representative's computer screen while on the customer service call. The number of audio files and video "screen shots" restored and reviewed has been very large, to say the least. There were over 1,000,000 voice audio files, and over 300,000 video "screen shot" files reviewed. Unfortunately, after checking with numerous vendors, an electronic solution could not be formulated, and a

New Hampshire, we will be issuing such a release in your state shortly

largely manual review of the audio and video files was necessary. BlueCross hired Kroll OnTrack to aid BlueCross in the data restoration and review. BlueCross also dedicated internal employees and hired temporary employees to aid in the review. Between BlueCross and Kroll, hundreds of staff spent approximately 107,000 hours reviewing the audio and video data.

BlueCross has assigned all of its potentially impacted members to one of three risk tiers. The lowest tier includes those members whose name, BlueCross Subscriber ID, date of birth, and/or address was present in the audio call or video screen shot. The second tier includes all of the aforementioned, plus diagnosis or diagnosis code. The third and highest risk tier includes those members with a social security number potentially at risk. BlueCross's first priority has been to notify members whose social security numbers may be at risk. If a member has been identified as having a social security number potentially at risk, they will receive a "Tier 3" notification letter. A copy of one version of our current Tier 3 notice letter is attached hereto.

To date, BlueCross has sent out approximately 238,589 Tier 3 letters which, again, began mailing on a rolling basis on December 7. We have also mailed approximately 146,612 Tier 2 letters which provide notice to approximately 311,000 Tier 2 members (subscribers and their dependents). Finally, there are approximately 400,000 members in Tier 1, and we expect our Tier 1 mailings to begin this week and be completed in the first full week of April.

The vast majority of all affected members reside in the State of Tennessee where we operate. Nonetheless, many of our large accounts do have employees that live in states other than Tennessee.

In our analysis, we have discovered numerous states which have over 500 members being notified. The federal HITECH Act requires that we provide media notice to any jurisdiction where over 500 members may reside; therefore, we are also notifying all Attorneys General in these states (including your office) so they may also be aware of our activities and could address questions they may potentially receive from our members who reside in their states following such a press release. Since we now have over 500 potentially affected members in the State of New Hampshire, we will be issuing such a release in your state shortly.

BlueCross's first priority is the notification and protection of our members, and we are working as quickly as we possibly can to accomplish that. In order to prevent any identity theft issues, we are offering to "Tier 3" members free credit monitoring through Equifax for one year, and Equifax's "3 in 1 Gold Credit Watch Program" which includes up to $1,000,000 in identity theft insurance. For minors, we have engaged LifeLock® to aid in monitoring both credit and noncredit sources, since the Equifax monitoring is not applicable to minors. In addition, for all members involved in the breach, regardless of Tier, we have hired Kroll to send out our notification letters and staff a telephone call center which provides access to Licensed Investigators who will speak with any member who has questions regarding identity theft or who thinks they may be a victim of identity theft. The Licensed Investigators can also access a proprietary database as a result of being Licensed Investigators in order to aid in determining whether there has been suspicious or fraudulent activity related to a member's identity. In addition, if any member has been a victim of identity theft as a result of this incident, BlueCross

investigation. We have also met with our local State District Attorney in order to hopefully move the investigation forward. If you have further questions regarding our current theft investigation, please do not hesitate to contact us and we will be happy to share them with you.

Also feel free to contact BlueCross's Deputy General Counsel, [redacted] or our outside counsel, who are also working with us on this matter, [redacted], who are both with the law firm of [redacted].

It is an understatement to say that BlueCross regrets this data breach. Please know that we will, however, continue to protect our members as best we can. Again, if we can answer any questions from you or anyone in your office, please do not hesitate to contact us.

With best regards, I am

Yours very truly,

Bill Young
Senior Vice President of Risk Management
and General Counsel

Enclosures
cc: Tennessee Attorney General Robert Cooper
Mr. Roosevelt Freeman, Regional Director, HHS-OCR – Via Email
Adam Greene, Office of Counsel to HHS, Civil Rights Division – Via Email
Chris Griffin, Assistant Regional Counsel to HHS – Via Email
Tena Roberson, Deputy General Counsel and Chief Privacy Officer - BlueCross
Brenda G. Wynkoop, Manager, Legal Compliance - BlueCross
Richard Rose, Esq. – Miller & Martin PLLC
Leah Gerbitz, Esq. – Miller & Martin PLLC

BlueCross BlueShield of Tennessee has also placed information on its Web site, www.bcbst.com, to provide its members with information regarding this theft. The Federal Trade Commission (FTC) has also released detailed information on steps you can take to protect against identity theft. You can find information on the FTC Web site at www.ftc.gov, or you can call 1-877-IDTHEFT (1-877-438-4338; TTY 1-866-653-4261).

BlueCross BlueShield of Tennessee's internal investigators are continuing to work with local and federal authorities on the investigation of the breach. BlueCross BlueShield of Tennessee is also obtaining an independent assessment of BlueCross BlueShield of Tennessee's system-wide data and facility security to continue to provide the best security possible.

We will continue to work with our members to address all concerns and provide information and assistance to ensure our members' needs are being met. If you have any questions or would like more information, please contact us at 1-888-422-2786 or Privacy_Questions_GM@bcbst.com.

BlueCross BlueShield of Tennessee deeply regrets this situation. BlueCross BlueShield of Tennessee has always been committed to taking measures to safeguard your information and we take privacy concerns very seriously.

Sincerely,

Brenda G. Wynkoop

Brenda G. Wynkoop
Manager, Legal Compliance
Privacy Office

Equifax Credit Watch Gold with 3-in-1 Monitoring Instruction Guide

Dear Member: We have arranged with Equifax Personal Solutions to help you protect your identity and your credit information at no cost to you. The steps to follow are:

1. Enroll in Equifax Credit Watch™ Gold with 3-in-1 Monitoring identity theft protection product. This product is being provided to you at no cost for one year.

2. Additionally, you may choose to adopt an increased level of protection by placing a fraud alert on your credit file at Equifax and the other two credit reporting agencies. Enroll in Equifax Credit Watch™ Gold with 3-in-1 Monitoring.

Equifax Credit Watch will provide you with an early warning system to changes to your credit file and help you to understand the content of your credit file at the three major credit reporting agencies. The key features and benefits are listed below.

Equifax Credit Watch provides you with the following benefits:

- Comprehensive credit file monitoring and automated alerts of key changes to your Equifax, Experian, and TransUnion credit reports.
- Wireless alerts and customizable alerts available.
- One 3-in-1 Credit Report and access to your Equifax Credit Report™.
- $1,000,000 in identity theft insurance with $0 deductible, at no additional cost to you.
- 24 by 7 live agent Customer Service to assist you in understanding the content of your Equifax credit information, to provide personalized identity theft victim assistance and in initiating an investigation of inaccurate information.
- 90 day Fraud Alert placement with automatic renewal functionality (available online only).

How to Enroll

To sign up online for online delivery go to www.myservices.equifax.com/tri.

1. Consumer Information: complete the form with your contact information (name, address and e-mail address) and click "Continue" button. The information is provided in a secured environment.

2. Identity Verification: complete the form with your Social Security Number, date of birth, telephone #s, create a User Name and Password, agree to the Terms of Use and click "Continue" button. The system will ask you questions about your credit report that only you should know. Please note that on December 6, 2009, the Promotion Code field will be added to this page and you will need to enter your code in the box provided.

3. Payment Information: During the "check out" process, enter the promotion code, provided on the first page of this letter, in the "Enter Promotion Code" box. After entering your code press the "Apply Code" button (which will zero out the price) and then the "Submit Order" button at the bottom of the page. (This code eliminates the need to provide a credit card number for payment.)

4. Order Confirmation: Click "View My Product" to access your 3-in-1 Credit Report and other product features.

To sign up for US Mail delivery, dial 1-866-937-8432 for access to the Equifax Credit Watch automated enrollment process. Note that all credit reports and alerts will be sent to you via US Mail only.

1. Promotion Code: You will be asked to enter your promotion code as provided at the top of your letter.

2. Customer Information: You will be asked to enter your home telephone number, home address, name, date of birth and Social Security Number.

3. Permissible Purpose: You will be asked to provide Equifax with your permission to access your credit file and to monitor your file. Without your agreement, Equifax can not process your enrollment.

4. Order Confirmation: Equifax will provide a confirmation number with an explanation that you will receive your Fulfillment Kit via the US Mail (when Equifax is able to verify your identity) or a Customer Care letter with further instructions (if your identity can not be verified using the information provided). Please allow up to 10 business days to receive this information.

Directions for placing a Fraud Alert

A fraud alert is a consumer statement added to your credit report. This statement alerts creditors of possible fraudulent activity within your report as well as requests that they contact you prior to establishing any accounts in your name. Once the fraud alert is added to your credit report, all creditors should contact you prior to establishing any account in your name. To place a 90 day fraud alert on your credit file, log into the Equifax Member Center and click on the fraud alert tab, visit www.fraudalerts.equifax.com or call our auto fraud line at 1-877-478-7625, and follow the simple prompts. Once the fraud alert has been placed with Equifax, a notification will be sent to the other two credit reporting agencies, Experian and Trans Union, on your behalf. Fraud alerts last 90 days unless you manually renew it or use the automatic fraud alert feature within your Credit Watch subscription. Insurance underwritten by member companies of American International Group, Inc. The description herein is a summary only. It does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for complete details of coverage and exclusions. This product is not intended for minors (under 18 years of age).

U.S. State Notification Requirements

For residents of *Hawaii, Iowa, Maryland, Michigan, Missouri, North Carolina, Oregon, Vermont, Virginia, West Virginia,* and *Wyoming*:
It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity. You may obtain a free copy of your credit report by contacting any one or more of the following national consumer reporting agencies:

Equifax
P.O. Box 740241
Atlanta, Georgia 30374
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 2000
Chester, PA 19022
1-800-888-4213
www.transunion.com

For residents of *Iowa*:
State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *Oregon*:
State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission.

For residents of *Maryland* and *North Carolina*:
You can obtain information from the Maryland and North Carolina Offices of the Attorneys General and the Federal Trade Commission about steps you can take to avoid identity theft.

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

North Carolina Office of the Attorney General
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-566-7226
www.ncdoj.com

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

For residents of *Massachusetts* and *West Virginia*:
It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft. You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent; however, using a security freeze may delay your ability to obtain credit.

To place a security freeze on your credit report, you need to send a request to a consumer reporting agency by certified mail, overnight mail, or regular stamped mail. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. The consumer reporting agency may charge a fee of up to $5.00 to place a freeze or lift or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and you have submitted a valid police report relating to the identity theft incident to the consumer reporting agency.

Equifax Security Freeze
P.O. Box 105788
Atlanta, Georgia 30348
www.equifax.com

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion (FVAD)
P.O. Box 6790
Fullerton, CA 92834-6790
www.transunion.com

Released Dec. 4, 2009

Contact: Mary Thompson, APR
(423) 535-7694

Editor's Note: BlueCross BlueShield of Tennessee has issued this press release as required by the Health Information Technology for Economic and Clinical Health Act ("HITECH Act"), Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (Pub. L. 111-5) and its implementing regulations.

HITECH Act Notice Regarding BlueCross Hard Drive Theft

CHATTANOOGA, Tenn. — On Monday, Oct. 5, 2009 at 10 a.m., BlueCross BlueShield of Tennessee, Inc. employees discovered a theft of computer equipment at a network closet located in its former Eastgate Town Center office location in Chattanooga, Tenn. The theft occurred Friday, Oct. 2, 2009 at approximately 6:13 p.m. BlueCross has established that the items taken include 57 hard drives containing data that was encoded but not encrypted.

The hard drives were part of a system that recorded and stored audio and video recordings of coordination of care and eligibility telephone calls from providers and members to BlueCross' former Eastgate call center located in Chattanooga. The hard drives that were stolen contained data that included protected health information data of some members of the health plan. This data included member names and identification numbers and, on some but not all recordings, a diagnosis/diagnosis code, date of birth and/or a Social Security number.

BlueCross immediately investigated the breach and strengthened the existing security measures at the Eastgate Town Center where space was being leased. BlueCross is obtaining an independent assessment of system-wide data and facility security.

BlueCross has placed information on its Web site www.bcbst.com to provide its members information about this theft. The information includes the link to the Federal Trade Commission Web site, www.ftc.gov, where members can find information on steps they can take to protect against identity theft. Members can contact the BlueCross Eastgate Response Customer Call Center at 1-888-422-2786 to find out more information.

- more -

The back-up data of the stolen hard drives were restored and an exhaustive inventory of all data included on the drives is being conducted by BlueCross and Kroll Inc., a global leader in data security. BlueCross is in the process of sending rolling written notification to members as soon as they are identified as being affected by the data theft. The notification letters, which will be mailed to current and former BlueCross members, will specify the particular call center number that members should call. For any members whose Social Security number is identified at risk, credit monitoring services will be provided free of charge - which also includes up to a million dollars in identity theft insurance.

BlueCross has also engaged the services of Kroll to carry out the member notifications and provide its Enhanced Identity Theft Consultation and Restoration Services. Kroll's Licensed Investigators are available to answer any questions or identity theft concerns. In addition, in the unlikely event a member sustained identity theft as a result of this incident, BlueCross would also provide Identity Theft Restoration service through Kroll.

BlueCross has notified the Secretary of the Department of Health and Human Services and the State of Tennessee. BlueCross has also placed a notice with all three credit bureaus regarding this theft.

If a member receives a notification letter, the member will then be directed to call one of the numbers below:

- BlueCross Eastgate Response Customer Call Center
  1-888-422-2786 / 1-866-779-0487
- Members whose Social Security number has been identified to be at risk
  1-866-599-7347
- mailto:Privacy_Questions_GM@bcbst.com

For up-to-date information related to the Eastgate theft visit the BlueCross Web site at www.bcbst.com.

About BlueCross

BlueCross BlueShield of Tennessee offers its clients peace of mind through affordable solutions for health and healing, life and living. Founded in 1945, the Chattanooga-based company is focused on reinventing the health plan for both its 3 million Tennessee-based members as well as consumers across the country. Through its personal health advocacy approach, BlueCross is developing patient-centric products and services that positively impact affordability, patient safety and quality. BlueCross BlueShield of Tennessee Inc. is an independent licensee of the BlueCross BlueShield Association. For more information, visit the company's Web site at www.bcbst.com

– END –