



**BlueCross BlueShield  
of Tennessee**

1 Cameron Hill Circle  
Chattanooga, Tennessee 37402

[www.bcbst.com](http://www.bcbst.com)

Bill Young  
Senior Vice President of  
Risk Management and  
General Counsel

Telephone: (423) 535-7218  
Fax: (423) 591-9259  
E-mail [bill\\_young@bcbst.com](mailto:bill_young@bcbst.com)

December 16, 2009

**VIA FEDERAL EXPRESS  
AND CERTIFIED MAIL**

The Honorable Attorney General Janet Mills  
Maine Office of Attorney General  
109 Sewall Street  
Burton Cross Building, 6<sup>th</sup> Floor  
Augusta, Maine 04333

RECEIVED  
DEC 21 2009

Dear General Mills:

I am General Counsel to BlueCross BlueShield of Tennessee, Inc. ("BlueCross"), and 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 which contained encoded, but not encrypted, information. BlueCross employees discovered the theft the following Monday, October 5, 2009, and immediately reported it to law enforcement. On December 4, 2009, we learned that information of some of our members who reside in the State of Maine may have been included on the stolen drives. Accordingly, we are providing this notice and account of what we know thus far to you. We will also be providing notice to the applicable residents of your state as soon as they are identified, on a rolling basis. Thus far we believe the breach may have impacted 39 of our members who are Maine residents.

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 also 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.

The hard drives contained recorded telephone calls between 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. In the initial two sets

Attorney General Janet Mills

December 16, 2009

Page 2

of audio, there were approximately 550,000 audio files reviewed, and over 300,000 video "screen shot" files reviewed. The current and last audio file set being reviewed by our outside consultant is estimated to be approximately another 600,000 audio files. Unfortunately, after checking with numerous vendors throughout the country, an electronic solution could not be formulated, and a largely manual review of the audio and video files has been necessary. BlueCross hired Kroll OnTrack, a leader in data recovery and computer forensics to aid BlueCross in the data restoration, compilation, and review. BlueCross also dedicated internal employees and hired temporary employees to aid in the review. Between BlueCross and Kroll, through the first week of December, there were approximately 500 full-time equivalents and 300 part-time workers reviewing both the audio and video files and performing data entry. The full-time employees worked on two different shifts six days a week. To date, all 300,000 video files have been reviewed and are being processed and deduplicated for member identification and notification, and approximately 550,000 audio files have been reviewed and are being processed. The third and final set of audio data is currently being reviewed by well over 400 full-time Kroll staff, but we do not yet have a schedule for completion from Kroll. We will have one shortly. Since finalizing the video review, Kroll OnTrack has currently shifted its complete staff to full-time audio review.

BlueCross is currently taking the data which it has reviewed as well as which Kroll has reviewed and is processing it through its internal computer system to identify the members at issue and provide appropriate notice. We have already begun the notification process for members identified, and after providing this Notice to you, will immediately begin notifying, on a rolling basis, residents of your state.

In the audio files, typically, a caller would provide simply a BlueCross subscriber ID, name, date of birth, and in some cases, a diagnosis or diagnosis code. It was atypical on the recorded telephone calls for social security numbers to be mentioned, but with some calls involving Medicare patients, the HIC number was mentioned, which is a combination of a social security number and letters. Social security numbers did show up with greater frequency, however, on the video screen shots.

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 is 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 our Notice letters is attached hereto. We still do not know the final number of members involved as Kroll OnTrack still has a large amount of audio data to review and is reviewing it as quickly as possible. Once reviewed, this data must also be processed and deduplicated for member notifications. To date, BlueCross has sent out approximately 50,000 Tier 3 letters. The 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 also discovered several states which will have over 500

Attorney General Janet Mills

December 16, 2009

Page 3

members being notified. The 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 so they may also be aware of our activities and could address questions they may receive from our members who reside in their states.

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 for our members, we are offering to those members whose social security number may be at risk 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. In addition, for members involved in the breach, including those whose social security number is at risk, 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 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 has contracted with Kroll to work with our members to restore the member's credit to pre-theft status. Obviously, BlueCross is hopeful these measures will not be necessary, but we believe these will protect our members. In addition, Kroll's Licensed Investigators and Restoration Services are available to any minors whose personal information may be at risk, and for whom typical credit monitoring services are not sufficient, because minors do not have credit files. Obviously, if a minor's identity is stolen as a result of this incident, like any other member, Kroll will assist in restoring the minor's identity to pre-theft status.

In addition to having access to Kroll's telephone call center, members can also call or email the BlueCross Privacy Office with questions they may have. The contact information for the BlueCross Privacy Office is included in the member notices, and BlueCross has also posted information on its website from the FTC on how to detect and prevent identity theft.

We are hopeful that with the remedial measures in place, any damage to any of our members will be nonexistent or limited. To the extent that anyone does suffer any damages or identity theft, then the Equifax insurance and Kroll's restoration services should remedy such damage. BlueCross is committed to doing whatever it takes to prevent any damage to its members, which remains our first priority.

Because the theft occurred at a rental space which BlueCross leased for training purposes, BlueCross is having a complete audit and assessment of its physical security performed in order to prevent such an occurrence from happening again. In addition, although the theft involved a physical theft, rather than a penetration into BlueCross's computer network, BlueCross has also hired Stephen Baird, a former Department of Defense Cybercrimes Agent who is now with Kroll, to perform penetration testing or "hacking" of BlueCross's network, website, and other areas. This will further strengthen our security system. We are determined to prevent any future thefts and potential dangers to our members, as well as the substantial financial damages which this theft has caused BlueCross.

Attorney General Janet Mills

December 16, 2009

Page 4

As required by the federal HITECH Act and its implementing regulations, member notices are being sent out on a rolling basis as soon as we identify a member or group of members affected. We have notified all three major credit bureaus of the theft, and we will follow up with additional notices to the credit bureaus once we have completed all member notices and then know the final distribution of member notices. We have also issued a press release in the State of Tennessee, and we intend to issue a press release in any state in which we have more than 500 members at issue. A copy of the HITECH-mandated press release that has already been issued in Tennessee is attached hereto. We have also attached a copy of BlueCross's webpage updates. The press release has also been posted on our webpage.

We have informed the Office of Civil Rights and HHS and our State's Attorney General, General Cooper, that we would not meet the mandatory 60-day HITECH deadline for notification to members, and we explained to them why that was the case (due to the sheer volume of data being reviewed). Again, we are working as quickly as possible and, as we have told HHS, OCR, we are more than willing to discuss any aspect of our investigation, restoration, notification, and remediation processes with enforcement authorities. We also want your questions to be fully answered.

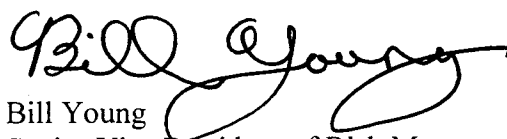
Finally, BlueCross has assigned two full-time internal investigators, which are former law enforcement officers and full-time employees of BlueCross, to investigate this theft. They are working with both the local Police Department and the FBI in connection with the investigation. If you have further questions regarding our current theft investigation, please do not hesitate to contact us and we will be happy to share them with you over the telephone rather than in this letter.

Also feel free to contact BlueCross's Deputy General Counsel, Tena Roberson, at 423-535-5158 or our outside counsel, who are also working with us on this matter, Richard Rose at 423-785-8268 or Leah Gerbitz at 423-785-8372, who are both with the law firm of Miller & Martin PLLC in Chattanooga, Tennessee.

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, and deal with the issues raised hereby in the most responsible and best way that 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

Attorney General Janet Mills

December 16, 2009

Page 5

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

Secure Processing Center | 600 Satellite Blvd | Suwanee, GA 30024

URGENT — Please Open Immediately.

<<FirstName>> <<MiddleName>> <<LastName>> <<Suffix>>  
 <<Address1>>  
 <<Address2>>  
 <<City>>, <<StateProvince>> <<PostalCode>>  
 <POSTNET BARCODE>

## ID TheftSmart™

<<FirstName>> <<MiddleName>> <<LastName>>  
 Membership Number: <<MembershipNumber>>

Member Services: 1-866-599-7347  
 8:00 a.m. to 7:00 p.m. (Central Time), Monday through Friday  
 If you have questions or feel you may have an identity theft issue,  
 please call ID TheftSmart member services.

<<Date (Month Day, Year)>>

Dear Member:

On Monday, October 5, 2009 at 10:00 a.m., BlueCross BlueShield of Tennessee, Inc. employees discovered a theft of computer equipment at a network closet located in our Eastgate Town Center office location in Chattanooga, TN. The theft occurred Friday, October 2, 2009 at approximately 6:13 p.m. BlueCross BlueShield of Tennessee has established that the items taken include 57 hard drives, containing data which was encoded but not encrypted.

The hard drives contained encoded audio and video recordings of member and provider eligibility and coordination of benefits calls to BlueCross BlueShield of Tennessee's Eastgate call center. As a current or former member, BlueCross BlueShield of Tennessee has identified that some of your information was stored on the hard drives and potentially could be accessed. The information potentially at risk includes your name, address, member ID, diagnosis code, Social Security number and/or date of birth.

While BlueCross BlueShield of Tennessee believes there is a low risk this information could be used inappropriately, we understand you could be concerned about unauthorized use of your personal information. BlueCross BlueShield of Tennessee suggests that you closely monitor your claim activities by carefully reviewing your explanation of benefits (EOB) statements from BlueCross BlueShield of Tennessee.

To mitigate the possibility of misuse of your information, BlueCross BlueShield of Tennessee has engaged Kroll, a global leader in data security, to provide its ID TheftSmart™ program for one year from the date of this notification. This program includes access to Kroll's Solution Support Center for questions about the event or identity theft concerns, as well as Enhanced Identity Theft Consultation and Restoration described below. Kroll's team has extensive experience when it comes to helping people who have experienced the unintentional exposure or potential exposure of confidential data. BlueCross BlueShield of Tennessee is providing you FREE access to:

- › **Enhanced Identity Theft Consultation and Restoration.** Kroll's Licensed Investigators, who truly understand the problems surrounding data breaches and identity theft, are available to listen, to answer your questions, and to offer their expertise regarding any concerns you may have. In the unlikely event that you were a victim of identity theft as a result of this incident, BlueCross BlueShield of Tennessee will further provide identity theft restoration services through which Kroll's Licensed Investigators will help restore your identity to pre-theft status. The investigators do most of the work.

You may call 1-866-599-7347, 8:00 a.m. to 7:00 p.m. (Central Time), Monday through Friday, if you have any questions or feel you may have an identity theft issue.

In addition, in an effort to prevent unauthorized use of your information, BlueCross BlueShield of Tennessee is offering you free credit monitoring for one year provided by Credit Watch Gold with 3-in-1 Monitoring by Equifax Personal Solutions. With Credit Watch Gold with 3-in-1 Monitoring, you will receive:

- › Comprehensive credit file monitoring of your credit reports through the three major credit reporting agencies
- › 24/7 live agent customer service to assist you in understanding your credit information and provide support in the investigation of any inaccurate information
- › \$1,000,000 in identity theft insurance with \$0 deductible, at no additional cost to you

Your Equifax activation code is <<ClientDef1>>. To sign up online for online delivery, please go to [www.myservices.equifax.com/tri](http://www.myservices.equifax.com/tri). To enroll for US Mail delivery, please call 1-866-937-8432. To learn more on how to activate and take advantage of this service, please review the information at the end of this letter.

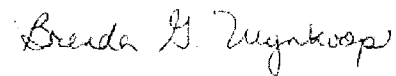
BlueCross BlueShield of Tennessee has also placed information on its Web site, [www.bcbst.com](http://www.bcbst.com), to provide its members with information regarding this theft. The Federal Trade Commission (FTC) has also released detailed information on steps you can take to protect against identity theft. You can find information on the FTC Web site at [www.ftc.gov](http://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](mailto: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  
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](http://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](http://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](http://www.equifax.com)

#### **Experian**

P.O. Box 2002  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com](http://www.experian.com)

#### **TransUnion**

P.O. Box 2000  
Chester, PA 19022  
1-800-888-4213  
[www.transunion.com](http://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](http://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](http://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/](http://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](http://www.equifax.com)

#### **Experian Security Freeze**

P.O. Box 9554  
Allen, TX 75013  
[www.experian.com](http://www.experian.com)

#### **TransUnion (FVAD)**

P.O. Box 6790  
Fullerton, CA 92834-6790  
[www.transunion.com](http://www.transunion.com)

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](http://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](http://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](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](http://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](http://www.bcbst.com).

– END –



**October 7, 2009**

### **Statement on Hard Drive Theft**

Over the weekend, unauthorized persons entered a data closet in a remote location that BlueCross BlueShield of Tennessee still leases for training purposes (Eastgate Town Center). They removed some computer equipment, including small hard drives containing encoded data.

BlueCross continues to work with local and federal authorities. Based on what we know so far in this investigation, the stolen computer equipment contained voice recordings of eligibility and coordination-of-benefit calls used for training purposes. The retrieval of member data from these drives would require highly-specialized expertise and software; therefore, at the present time, we have no reason to believe that member data has been accessed.

Reports of a burglar alarm that went off Friday evening at the Eastgate Town Center location are inaccurate. On Friday evening Oct. 2, our computer monitoring systems generated a notice that there was an issue with the servers in the data closet. This electronic notice only indicated that the servers were not functioning properly, not that there had been a theft from the server room. As these servers were not critical to our operations during the weekend, we did not dispatch an employee until Monday morning. On Monday morning an information systems employee went to physically service the equipment only to discover then that the disk drives had been stolen.

BlueCross takes the security of our members' health information seriously. If we discover that any members' personal information has been compromised, we will reach out directly to notify those members as soon as possible. We have a team working diligently to determine what personal information, if any, has been accessed.

As details become available, BlueCross will post that information on its Web site, [bcbst.com](http://www.bcbst.com).

BlueCross BlueShield of Tennessee does not make unsolicited phone calls asking for personal information such as bank account or drivers license information.

#### **About BlueCross**

BlueCross BlueShield of Tennessee is the state's oldest and largest not-for-profit health plan, serving nearly 3 million Tennesseans. Founded in 1945, the Chattanooga-based company is focused on financing affordable health care coverage and providing peace of mind for all Tennesseans. BlueCross serves its members by delivering quality health care products, services and information. BlueCross BlueShield of Tennessee Inc. is an independent licensee of BlueCross BlueShield Association. For more information, visit the company's Web site at [www.bcbst.com](http://www.bcbst.com).

---

**[Return to Press Releases](#)**



October 15, 2009

### Statement on Hard Drive Theft (Update)

BlueCross BlueShield of Tennessee is committed to maintaining high levels of security for all our members and we acknowledge that the recent theft of 57 hard drives has caused concern. We apologize and want our members and groups to know that we will continue to work to address all concerns, as well as provide information and assistance to ensure we are meeting our customers' needs.

BlueCross has undertaken the following measures:

- We have an internal team of IT experts working diligently to assess the information contained on the hard drives using our system backup tapes. Those efforts are being assisted by Kroll Ontrack®, a leading national provider of data recovery and security solutions.
- We continue to work with local and federal authorities on the criminal investigation.
- We have reviewed and reinforced physical security measures at all company-owned and leased properties by adding additional video camera surveillance, reviewing our biometric and key card access readers, and increasing our security personnel presence.
- We are complying with all applicable state and federal laws, including the the HITECH Act of 2009.
- We will be retaining an independent third party firm to perform a security assessment so we can further strengthen our existing security.

Our current focus is identifying the clients who potentially have members whose information could be contained on the stolen hard drives. We expect it will take several weeks to identify affected clients, as the process requires the need to listen to each recorded phone call.

Once identified, the clients will be notified via priority mail that they have had members whose personal information is contained in the stolen records and therefore at risk.

Next steps will involve an exhaustive process of identifying the specifically impacted members. These members will receive notice of the information that was contained on the stolen hard drives. We anticipate that this process may take up to 60 days for a full assessment of the information.

BlueCross clients and members who may have additional questions or concerns may contact the BlueCross Privacy Office Hotlines at 1-888-422-2786 or 1-888-455-3824 or send an email to [Privacy\\_Office@bcbst.com](mailto:Privacy_Office@bcbst.com).

BlueCross BlueShield of Tennessee does not make unsolicited phone calls asking for personal information such as bank account or drivers license information.

#### About BlueCross

BlueCross BlueShield of Tennessee is the state's oldest and largest not-for-profit health plan, serving nearly 3 million Tennesseans. Founded in 1945, the Chattanooga-based company is focused on financing affordable health care coverage and providing peace of mind for all Tennesseans. BlueCross serves its members by delivering quality health care products, services and information. BlueCross BlueShield of Tennessee Inc. is an independent licensee of BlueCross BlueShield Association. For more information, visit the company's Web site at [www.bcbst.com](http://www.bcbst.com).

---

[Return to Press Releases](#)



**November 23, 2009**

### **Hard Drive Theft Investigation, Analysis Continues**

BlueCross BlueShield of Tennessee continues to investigate the Oct. 2 hard drive theft that occurred in a data closet at its remote training facility in Chattanooga. We are working closely with local, state and federal authorities in their investigation of this crime.

We want to thank our group customers and our members for their patience as we tirelessly analyze the backup tapes of the stolen data. This is a very cumbersome and complex process that we have committed our full resources to. We have over 800 staff from BlueCross, a temporary staffing service and our data security contractor working six days a week retrieving and reviewing back up files. This team is combing through 300,000 screen image files and reviewing 50,000 hours of audio recordings stored on the stolen drives to determine the exact data at risk.

On Nov. 20, letters to group administrators were mailed out informing our employer groups precisely how we are handling the notification to our impacted members. We anticipate that we will begin notifying affected members by mail beginning Nov. 30, with notifications occurring progressively over several weeks. Any members who are found to have had their Social Security number included in the data will be provided free Equifax credit monitoring for a year.

We realize that this issue has caused much concern for our brokers, groups and members, and we want to provide assurance that the protection of personal health information is a top priority for us.

Questions regarding this data security issue or other privacy matters may be directed to the BlueCross BlueShield of Tennessee Privacy Office Hotlines at 1-888-422-2786 or 1-888-455-3824 or via email at [Privacy\\_Office@bcbst.com](mailto:Privacy_Office@bcbst.com).

BlueCross BlueShield of Tennessee does not make unsolicited phone calls asking for personal information such as bank account or drivers license information.

#### **About BlueCross**

BlueCross BlueShield of Tennessee is the state's oldest and largest not-for-profit health plan, serving nearly 3 million Tennesseans. Founded in 1945, the Chattanooga-based company is focused on financing affordable health care coverage and providing peace of mind for all Tennesseans. BlueCross serves its members by delivering quality health care products, services and information. BlueCross BlueShield of Tennessee Inc. is an independent licensee of BlueCross BlueShield Association. For more information, visit the company's Web site at [www.bcbst.com](http://www.bcbst.com).

---

**[Return to Press Releases](#)**