



of Tennessee

plans for better health. plans for a better life.™

1 Cameron Hill Circle
Chattanooga, TN 37402

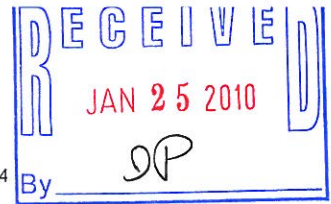
bcbst.com

Privacy Office

Telephone (888) 455-3824

Fax 1-423-535-1976

E-mail Privacy_Office@bcbst.com



January 14, 2010

City of Franklin
109 3rd Ave S
Franklin TN 37064-2519

Dear Group Administrator,

Over the course of the past 90 days, BlueCross BlueShield of Tennessee has been diligently reviewing and analyzing the backup files of the stolen hard drives taken from Eastgate Town Center location on October 2, 2009. Since early December, nearly 200,000 active and former members have been identified on those files and notified that certain personal information was included on the stolen hard drives. That information included the member's name, address, BlueCross BlueShield of Tennessee member ID, diagnosis, Social Security number and/or date of birth. Letters have been sent to those members offering identity protection and restoration services, along with specific information on steps the member can take to protect their own personal information.

On October 6, 2009, BlueCross BlueShield of Tennessee began communicating to brokers and employers of this incident and has been providing periodic updates as more information became available. Additionally, BlueCross BlueShield of Tennessee has delivered press and media releases in order to keep members, brokers and employers informed of the progress of the investigation and efforts to quickly identify and notify members of the potential of their data being accessed. Those releases have gone out on a national level to comply with state and federal guidelines, as well as ensuring that all of BlueCross BlueShield of Tennessee's nearly 3 million members are aware of the theft.

As of January 4, 2010, we have completed the audit of the 1.3 million audio files and 300,000 video files and will now begin a broad communications effort to members, brokers and employers providing details of total affected members and our notification and remediation steps. We will continue to post regular updates to our Web site, bcbst.com – including a special **Eastgate Hard Drive Theft** page – along with a FAQ section to assist in providing answers to many questions we have received over the past few weeks.

Part of this comprehensive communications effort is to provide more detail on the steps BlueCross BlueShield of Tennessee has taken to identify and protect the personal data of affected members. Beginning with the member notification letters generated the week of January 11, 2010, information will be included regarding the discovery of the theft of the hard drives and BlueCross BlueShield of Tennessee's response to that incident. Additionally,

BlueCross BlueShield of Tennessee members that are classified as minors will be receiving a specific notification letter addressed to their parent or guardian and offering LifeLock Identity Alert™ services. Samples of all member letters have been included for you to review.

As always, we value the trust you place in BlueCross BlueShield of Tennessee, and we will continue to provide timely and consistent communications as we work to bring final resolution to this incident. In the meantime, if you have any questions, please contact our Privacy Office at one of the numbers listed above. Or, you can visit our Web site at bcbst.com.

Sincerely,

A handwritten signature in black ink, appearing to read "Tena Roberson". The signature is fluid and cursive, with a long horizontal flourish extending to the right.

Tena Roberson
Deputy General Counsel and Chief Privacy Officer
BlueCross BlueShield of Tennessee

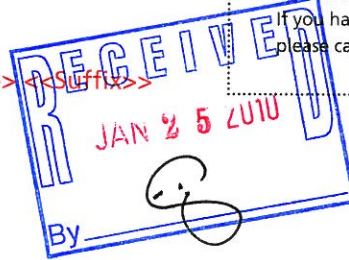


**BlueCross BlueShield
of Tennessee**

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

URGENT — Please Open Immediately.

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



<<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 Parent or Guardian:

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. BlueCross BlueShield of Tennessee has identified that some of your child's/dependent's, <ChildFirstName>, information was stored on the hard drives and potentially could be accessed. The information potentially at risk includes your child's/dependent's name, address, member ID, diagnosis, Social Security number and/or date of birth.

Upon learning of the theft, BlueCross BlueShield of Tennessee immediately investigated the crime and strengthened the existing security measures at the Eastgate Town Center where space was being leased. BlueCross BlueShield of Tennessee is obtaining an independent assessment of system-wide data and facility security.

BlueCross BlueShield of Tennessee and its consultant, Kroll, a global leader in data security, have been working tirelessly since the theft to review the back up tapes of the audio and video files, and to identify potentially impacted members. Hundreds of people have been working on multiple shifts, six days a week, to inventory the data contained on the files in order to notify members. Even with the large number of people reviewing the back up tapes, due to the sheer volume of the data, the process is taking time. BlueCross BlueShield of Tennessee and its consultant are working as quickly as possible to notify all members at issue.

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 this personal information. BlueCross BlueShield of Tennessee suggests that you closely monitor your child's/dependent's claim activities by carefully reviewing your explanation of benefits (EOB) and monthly claims statements from BlueCross BlueShield of Tennessee.

To mitigate the possibility of misuse of your child's/dependent's information, BlueCross BlueShield of Tennessee has engaged Kroll 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 child's/dependent's identity to pre-theft status. The investigators do most of the work.

Please note: Kroll and LifeLock are not in any way affiliated—they are separate service providers chosen by BlueCross BlueShield of Tennessee. You must contact each individually to take advantage of these separate services.

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, to help protect your child/dependent from future risk, BlueCross BlueShield of Tennessee has engaged LifeLock, a leader in identity theft protection, to provide you a one-year free LifeLock® for Children membership. LifeLock® services are designed to help stop identity thieves from misusing your child's/dependent's good name. With this FREE membership, LifeLock:

- > Alerts you when the LifeLock Identity Alert™ system detects your child's/dependent's personal information being used to apply for many more forms of credit and services (including credit cards, wireless services, utilities, and more).
- > Requests your child's/dependent's three free annual credit reports so you can monitor for potential problems.
- > Sends a form for you to request a copy of your child's/dependent's Earnings Report from the Social Security Administration. This report will allow you to check for fraudulent work and earnings histories that may result from compromised information.
- > Aids you in cancelling or replacing the contents of your child's/dependent's wallet should it be lost or stolen.
- > Gives you peace of mind with LifeLock's \$1 Million Total Service Guarantee. As a member of LifeLock, if your child/dependent becomes a victim of identity theft due to a failure in LifeLock® service, LifeLock will help fix it at their expense, up to \$1,000,000. (Restrictions apply. See lifelock.com for details.)

To begin protecting your child/dependent immediately, visit www.lifelock.com or call 1-877-509-5357 and use your LifeLock promotion code, **BCBST**, and your unique Member ID, <ClientDef1>. LifeLock is available 24 hours a day, seven days a week to assist you and your family.

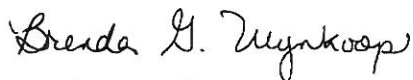
BlueCross BlueShield of Tennessee has also placed information on its Web site, www.bcbst.com, to provide its members with information regarding this theft. The Federal Trade Commission (FTC) has also released detailed information on steps you can take to protect against identity theft. You can find information 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
Manager, Legal Compliance
Privacy Office



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>



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

Member Services: 1-866-779-0487
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. <ClientDef1(Breach Details Variable Text)>(This field should be able to contain two lines of copy the same width of the body copy of the letter.)

Upon learning of the theft, BlueCross BlueShield of Tennessee immediately investigated the crime and strengthened the existing security measures at the Eastgate Town Center where space was being leased. BlueCross BlueShield of Tennessee is obtaining an independent assessment of system-wide data and facility security.

BlueCross BlueShield of Tennessee and its consultant, Kroll, a global leader in data security, have been working tirelessly since discovery of the theft to review the back up tapes of the audio and video files, and to identify potentially impacted members. Hundreds of people have been working on multiple shifts, six days a week, to inventory the data contained on the files in order to notify members. Even with the large number of people reviewing the back up tapes, due to the sheer volume of the data, the process is taking time. BlueCross BlueShield of Tennessee and its consultant are working as quickly as possible to notify all members at issue.

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, BCBST 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 1-866-779-0487, 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.

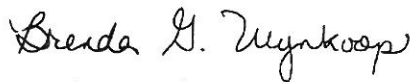
BlueCross BlueShield of Tennessee has also placed information on its Web site, www.bcbst.com, to provide its members with information regarding this theft. The Federal Trade Commission (FTC) has also released detailed information on steps you can take to protect against identity theft. You can find information 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
Manager, Legal Compliance
Privacy Office



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>



<<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.

Upon learning of the theft, BlueCross BlueShield of Tennessee immediately investigated the crime and strengthened the existing security measures at the Eastgate Town Center where space was being leased. BlueCross BlueShield of Tennessee is obtaining an independent assessment of system-wide data and facility security.

BlueCross BlueShield of Tennessee and its consultant, Kroll, a global leader in data security, have been working tirelessly since discovery of the theft to review the back up tapes of the audio and video files, and to identify potentially impacted members. Hundreds of people have been working on multiple shifts, six days a week, to inventory the data contained on the files in order to notify members. Even with the large number of people reviewing the back up tapes, due to the sheer volume of the data, the process is taking time. BlueCross BlueShield of Tennessee and its consultant are working as quickly as possible to notify all members at issue.

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) and monthly claims statements from BlueCross BlueShield of Tennessee.

To mitigate the possibility of misuse of your information, BlueCross BlueShield of Tennessee has engaged Kroll 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 promotion code is <<ClientDef1>>. To sign up online for online delivery, please go to 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.

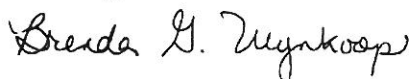
BlueCross BlueShield of Tennessee has also placed information on its Web site, www.bcbst.com, to provide its members with information regarding this theft. The Federal Trade Commission (FTC) has also released detailed information on steps you can take to protect against identity theft. You can find information 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
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 at the top of the second 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 page two.
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).