


 search

## Eastgate Hard Drive Theft

### EASTGATE HARD DRIVE THEFT

**Background--Last updated January 13, 2010**

In October 2009, 57 hard drives containing audio and video files related to coordination of care and eligibility telephone calls from providers and members were stolen from a leased facility in Chattanooga that formerly housed a BlueCross BlueShield of Tennessee call center. The video files were images from computer screens of BlueCross customer service representatives and the audio files were recorded phone conversations from January 1, 2007 to October 2, 2009.

The files contained BlueCross members' personal data and protected health information that was encoded but not encrypted, including:

- Members' names and BlueCross ID numbers
- In some recordings – but not all – diagnostic information, date of birth and/or a Social Security number

BlueCross immediately investigated the theft and continues to work closely with local and federal authorities in their investigation of this crime. In addition, BlueCross hired Kroll, a global leader in security services, to conduct an independent assessment of its system-wide security and has taken several actions to strengthen these protocols.

**Scope of Risk**

BlueCross is committed to protecting its customers' personal information and takes seriously any risks associated with this crime. BlueCross believes there is minimal risk to members' data being accessed due to the specialized nature of the hardware stolen and the difficulties associated with accessing the stored data.

Law enforcement agencies working on the investigation of the theft are regularly monitoring activity on Web sites known to participate in illegal identity theft activities, as well as online marketplace and community networks. To date, there is no evidence any member's data has been accessed and used as a result of the theft.

**Our Response Process**

BlueCross had backup files of all stolen data and began working with [Kroll](#) as soon as the theft was discovered in October to review files and identify members whose personal information may be at risk.

Due to the amount and types of the data involved, it is taking significant time to review each recording. BlueCross is working as quickly as possible to notify all affected members. As of January 7, 2010, more than 110,000 hours were logged during this effort to identify members at-risk.

Estimated\* audio files stolen: 1,300,000  
 Estimated\* video files stolen: 300,000  
 Estimated\* number of BlueCross members at risk: 500,000

\*Final numbers will be available at completion of file review

Three levels of risk have been identified for those members whose information may be at risk. Letters are being mailed to these current and former BlueCross members explaining the level at which their personal information is at risk. Members are being offered a variety of free services to mitigate the potential for misuse of personal information.

RISK LEVEL	DESCRIPTION OF RECORDING DATA	# IDENTIFIED AS OF 10/8/09	# NOTIFIED BY MAIL SINCE 12/7/09	REMEDATION OFFERED
Tier 3	Member's name,	220,000	157,482	■ Free credit monitoring for one year provided by

90%  
 Complete  
 On Data  
 Matching

<b>RISK LEVEL</b>	<b>DESCRIPTION OF RECORDING DATA</b>	<b># IDENTIFIED AS OF 10/8/09</b>	<b># NOTIFIED BY MAIL SINCE 12/7/09</b>	<b>REMEDATION OFFERED</b>
-------------------	--	---------------------------------------	---	---------------------------

\* For BlueCross members identified as minors

Members who have questions or want more information should call the BlueCross Eastgate Response Customer Call Center at 1-888-422-2786 or can email [Privacy\\_Questions\\_GM@bcbst.com](mailto:Privacy_Questions_GM@bcbst.com). Recommendations to protect against identity theft are available at [www.ftc.gov](http://www.ftc.gov).

#### ***Locations of Members At Risk***

While most BlueCross members reside in Tennessee, the company has membership in all 50 states. As of January 8, 2010, BlueCross has identified 32 states with 500 or more members whose data may be at risk. BlueCross notifies the Secretary of the Department of Health and Human Services, the State of Tennessee and the attorney general's office and media in each state with 500 or more affected members, as required by the Health Information Technology for Economic and Clinical Health Act ("HITECH Act") and its implementing regulations. BlueCross has also placed a notice with all three credit bureaus regarding this theft. At-risk members are strongly encouraged by BlueCross to take full advantage of the pre-paid protection services offered in their notification letter. [Click here](#) for FAQs.

© 1998-2009 BlueCross BlueShield of Tennessee, Inc., an Independent Licensee of the BlueCross BlueShield Association. ® Registered marks of BlueCross BlueShield Association. 

Page Modified: January 21, 2010