HISTORIC
FRANKLIN
TENNESSEE

ITEM #13
WRK S 02/09/10

MEMORANDUM

January 27, 2010

TO: Board of Mayor and Aldermen

FROM: Eric S. Stuckey, City Administrator
Shirley Harmon, Human Resources Director
Rodney Escobar, Risk Manager

SUBJECT: Annual Report for the City of Franklin's FACTA Program (identity theft prevention)

Purpose

The purpose of this memorandum is to present to the Board of Mayor and Aldermen (BOMA) an annual report as required under the Fair and Accurate Credit Transactions Act (FACTA), a program designed to provide identity theft prevention for consumers.

Background

FACTA is Federal legislation adopted in 2003 and amended in 2009 that provides for identity theft prevention for consumers. From the City's perspective, FACTA outlines certain municipal departments to enact certain policies and procedures called "Red Flag" rules. As part of this legislation and the BOMA-approved policy, an annual report must be provided to the Board. The report will address material matters related to the FACTA Program and evaluate issues such as: the effectiveness of policies and procedures in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts; service provider arrangements; significant incidents involving identity theft and management's response; and recommendations for material changes to the program.

Financial Impact

If the city fails to comply with this regulation any FACTA violation will be subject to civil monetary penalties up to $2,500 for every violation (federally), state fines up to $1,000 per incident, and damage to the City's image and reputation.

Options

This is a federal mandated requirement.

Recommendation

It is recommended that BOMA accept the FACTA annual report in accordance with legal requirements and Board policy.

Identity Theft Prevention Program Annual Report
City of Franklin Board of Mayor and Alderman

January 22, 2010

The intent of this report is to provide the overall status of the Identity Theft Prevention Program, along with providing any updates to any of the program components.

Status

The Identity Theft Prevention Program was last updated on January 11, 2010. The overall status of the Identity Theft Prevention Program is very good.

Effectiveness of Policies and Procedures

City of Franklin has implemented appropriate policies and procedures to comply with 16 CFR Part 681 (Identity Theft Red Flags) to address the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered account.

See Identity Theft Prevention Program provided separately.

Service Provider Arrangements

1. New service providers
    a. Risk Manager has drafted a Service Provider Agreement between the City of Franklin and vendors that receive identifying information from the City for official City business and benefit programs.
2. Changes in vendor management processes, procedures, or requirements
    a. The only changes with vendor management process is to have all new and current vendors sign the Service Provider Agreement. A copy of the drafted agreement has been sent to the City Law Department for review. (Please see the attachment of the Service Provider Agreement for further details).

Significant Incidents Involving Identity Theft and Management Response

1. Any significant incidents involving identity theft this year and action taken?
    a. There were no reported significant incidents involving identity theft in 2009 for the internally for the City of Franklin.
2. Any service provider significant incidents involving identity theft this year and action taken?

a. On October 2, 2009, Blue Cross Blue Shield of Tennessee reported to the City of Franklin a theft of their computer equipment at a network office, located at Eastgate Town Center in Chattanooga, Tennessee. The theft of the equipment included 57 hard drives, containing data which was encoded but not encrypted. (Please, see attached letter from Blue Cross Blue Shields for further details).

Recommendations for Changes in the Identity Theft Prevention Program

1. Additions to the Identity Theft Prevention Program?
    a. Continue online training for FACTA.
    b. Adopt the practice of having new and current service providers sign the Service Provider Agreement for the City of Franklin.
2. Deletions from the Identity Theft Prevention Program
    a. None.

Rodney Escobar

From: Tammie Pitts
Sent: Tuesday, January 26, 2010 3:25 PM
To: Rodney Escobar
Subject: FW: Eastgate Hard Drive Theft Update

Rodney, please see the communication below from BCBST concerning the October data theft.

Thanks,

Tammie Pitts, PHR
Benefits Manager
City of Franklin
109 3rd Avenue South
Franklin, TN 37064
Phone: (615) 791-3223
Fax: (615) 550-1965

From: Harding, Connie [mailto:Connie_Harding@BCBST.COM]
Sent: Tuesday, January 26, 2010 2:12 PM
To: MKTNASHTEL-L@LISTSERV.BCBST.COM
Subject: Eastgate Hard Drive Theft Update

During the past two weeks, significant progress has been made in BlueCross BlueShield of Tennessee's continuing auditing, identifying and notification efforts of members affected by the Eastgate hard drive theft.

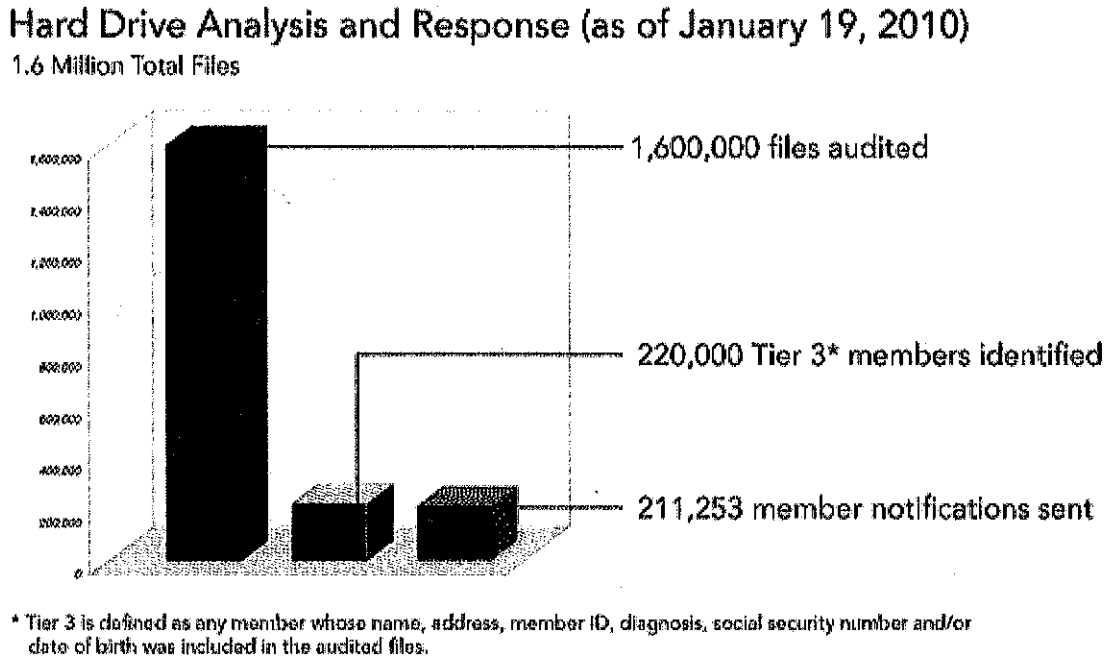
As of January 19, 2010, 220,000 current and former members have been identified and 211,253 notifications have been sent to members indicating that their personal information was included on the stolen hard drives and have been offered remediation services, including credit monitoring and identity theft protection. These members, which fall in the Tier 3 category, have been confirmed as having their name, address, BlueCross member ID number, diagnosis, Social Security number and/or date of birth included in the stolen hard drives. Additionally, minors whose personal information has been identified in the Tier 3 category have begun to receive letters offering LifeLock® identity services.

BlueCross has confirmed that 20,940 members have contacted Equifax to initiate the free 3-in-1 credit monitoring service offered to those members in the Tier 3 category. Also, two members have contacted Kroll regarding activation of its Enhanced Identity Theft Consultation and Restoration services. However, as of January 19, 2010, there has been no documented incident of identity theft or credit fraud of BlueCross members as a result of this incident.

Beginning in early February, members falling in the Tier 2 category of personal information (name, address, BlueCross member ID number and diagnosis) will begin to receive their notifications with details of the hard drive theft and

remediation services offered to them.

Below is a graphical representation of total members identified and notifications sent as of January 19, 2010. If you are unable to view this image, you can go to the Eastgate Hard Drive Theft page of bcbst.com to view this statistic and other information related to our identification and notification efforts.



While this theft has received significant coverage in many Tennessee news and media outlets, our auditing and notification process has received favorable reviews from IT-related online publications and blogs. BlueCross has been lauded for its open and frequent communications, as well as engaging a leader in data security, Kroll, in assisting with its file audit and remediation efforts.

BlueCross BlueShield of Tennessee is committed to delivering up-to-date and relevant communications to its clients – members, brokers and employers – as information becomes available. As always, you can direct questions specific to this incident to the BlueCross BlueShield of Tennessee Privacy Office by calling 1-888-422-2786 or through email at Privacy_Questions_GM@bcbst.com. Or, you can visit our Web site at bcbst.com.