Visionworks

November 11, 2014

The Honorable Tom Miller
ATTN: Consumer Protection Division
1305 E. Walnut Street
Des Moines, IA 50319

Dear Mr. Attorney General:

This letter is to inform you of a recent incident that involved the loss of the Personal Information ("PI") and/or Protected Health Information ("PHI") of two (2) of your state's residents.

As part of a multi-step initiative to fully encrypt the servers at all of our locations, a scheduled server replacement was performed on June 2, 2014 in our Visionworks store at Jennifer Square, 169 Jennifer Road, Annapolis, Maryland. Following the replacement, the partially encrypted decommissioned server was placed in a box and stored temporarily in the in-store lab until it was recalled and shipped back to the San Antonio home office. On October 27, 2014, the server was recalled, and it was discovered that it was missing from the store.

An investigation immediately ensued which revealed that a remodel of the store began on June 15, 2014, shortly after the server replacement. The investigation further revealed that significant amounts of construction material and debris was removed from the store and disposed of in construction dumpsters during that time. Although we are unable to conclusively confirm, all of the facts of the investigation suggest, and we strongly suspect, that the server was placed into the dumpster used for construction waste by either an employee or contractor. We have every reason to conclude that the server is now buried in a local landfill.

Our investigation further revealed that the server's hard drive contained fewer than 100 records of encrypted credit cardholder data ("CHD") which was stored for three (3) days from the time of the transaction (i.e., the encrypted, unreadable CHD impacted includes data from May 31, 2014, through June 2, 2014, when the server was decommissioned). The server's hard drive also contained unencrypted PI and PHI from the store's opening in 1997 through June 2, 2014. There was no customer data on this server after June 2, 2014.

As part of the investigation, we have attempted to identify the types of unencrypted data on the server. The missing data included the following data elements: name; address; home and work telephone numbers; health insurance information, including group name, group number, vision care expiration date and a member ID with up to 13 digits; date of birth; gender; occupation; referral source; service type and purpose of the visit; date of last visit; current balance; patient status; work order information, including examination information, comments and several eye glass frame, optical prescription and production related fields; and encrypted CHD.

There were also two Social Security Number ("SSN") fields available in the database; however, those fields were not populated. In some very limited cases, the member ID field may contain a SSN embedded within the full member ID; however, the field was not labeled as a SSN, and there is no reason to believe that anyone would identify this number as containing a SSN.

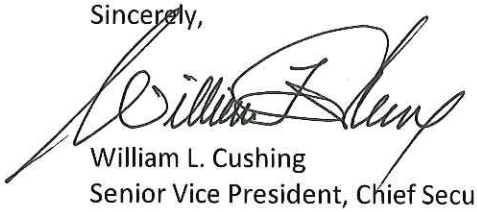
Our risk analysis concludes that the risk to this information is extremely low, and we have no evidence that any of the lost data has been accessed or used inappropriately; however, we elected to alert you and the affected individuals due to the nature of the information involved and out of an abundance of caution. Additionally, we will be offering free credit monitoring for one year to the affected individuals to mitigate any risks of identity theft. Enclosed, please find a copy of the letter Visionworks plans to send to your residents who were affected by this incident. To ensure these individuals receive notification as expediently as possible, while also ensuring that the notices are produced and mailed accurately, it is anticipated that the letters will be sent no later than November 21, 2014.

Impacted individuals may enroll in the Equifax credit monitoring program. Visionworks has also established a call center where individuals may call with questions related to this incident. The call center number is 1-888-778-7161. Additionally, you can read more about this incident at www.visionworks.com where Visionworks has placed a notice to alert those individuals who received services at the Jennifer Square, Annapolis, Maryland store of this incident.

We sincerely regret this incident and want to assure you that the privacy and security of information in Visionworks's possession is paramount to us. As such, we are continuing to work on our multi-step server encryption initiative to ensure that this type of incident doesn't occur in the future.

If you have any questions concerning this incident, or any matter relating to privacy, please call me.

Sincerely,



William L. Cushing
Senior Vice President, Chief Security Officer
HVHC, Inc.
175 E. Houston Street
San Antonio, Texas 78205
210-524-6962
bcushing@hvhc.com

Enclosure

cc: Jim Eisen, President, Visionworks, Inc.
Lisa A. Martinelli, Vice President, Chief Privacy Officer, Highmark Health

Visionworks

November 13, 2014

Activation Code: XXXXXXXXXXX

Dear xxxx,

At Visionworks we value your privacy, and we take steps to ensure that confidential information you provide to us is protected and kept secure. Unfortunately, we need to inform you of an incident that occurred recently that may affect you.

As part of an initiative to fully encrypt servers at all of our Visionworks locations, a scheduled server replacement was performed on June 2, 2014 at our Jennifer Square, Annapolis, Maryland location. The old server was placed in a shipping box and stored temporarily in the store until it was to be recalled to the San Antonio home office. However, on October 27, 2014, when the server was recalled, it was discovered that the server was missing.

A thorough investigation was immediately initiated. The investigation revealed that this store was remodeled shortly after the scheduled server replacement. During the course of the extensive remodel, significant amounts of construction material and debris was removed from the store and disposed of in construction dumpsters. Although we were unable to conclusively confirm, all of the facts of the investigation suggest, and we strongly suspect, that the server was placed into the dumpster by either a Visionworks employee or a contractor assisting with the remodel. We have every reason to conclude that the server is now buried in a local landfill.

The server's hard drive contained unencrypted personal information ("PI") and protected health information ("PHI"). The database stored on the missing server included fields for the following data elements: name; address; home and work telephone numbers; health insurance information, including group name, group number, vision care expiration date and a member ID; date of birth; gender; occupation; referral source; service type and purpose including examination information, comments and several fields related to eye glass frames, optical prescription and production related fields. Not all customers had information populated in every field included in the database. The hard drive also contained fewer than 100 records of fully encrypted, unreadable credit card data from the dates of May 31, 2014 through June 2, 2014, when the server was decommissioned. Encrypted credit card data was only stored for three (3) days.

Two Social Security Number ("SSN") fields were also available in the database. However, we were able to confirm that, in all cases, those fields were not populated. In some very limited cases, the member ID field contained a SSN embedded within the full member ID. This field was not labeled as an SSN, and there is no reason to believe that anyone would identify this number as containing a SSN.

Although we have no reason to believe that any of your information has been inappropriately accessed or misused and doubt that there is any reasonable risk of harm to you or your information, we nonetheless recommend that you remain vigilant by reviewing your account statements and monitoring credit reports. You should also report any incidents of suspected identity theft to us, the Federal Trade Commission, and to the proper law enforcement authorities. For additional information on how to protect your personal information and protect against identity theft, you can visit www.ftc.gov/idtheft or call 1-877-IDTHEFT (1-877-438-4338; TTY 1-866-653-4261).

Also, in order to provide you with an added level of security, Visionworks is offering you free credit monitoring for one year, provided by Equifax, to assist you in monitoring your information. Please see the enclosed insert for complete instructions on how to enroll in Equifax Credit Watch™ Gold identity theft protection.

To take advantage of this free offer, you need to enroll prior to February 1, 2015. This free credit service expires 12 months from the date you enroll with Equifax. You will also need the activation code that is printed at the top of this letter. So please keep this letter nearby when you go online or call to enroll. Additional information about Equifax Credit Watch Gold is available on their website.

If you have questions not related to the Equifax credit monitoring service, please call the Visionworks call center at 1-888-778-7161. Additionally, you can read more about this incident at www.visionworks.com.

Please be assured that Visionworks sincerely regrets any concern or inconvenience this incident may cause you. As a result of this incident, and in order to help prevent this type of incident from occurring in the future, in addition to continuing to pursue our server encryption initiative, Visionworks will initiate a thorough review of our policies and procedures regarding asset management in order to identify any methods by which we may further enhance our ability to protect your personal information.

Sincerely,

Jim Eisen

Jim Eisen
President
Visionworks of America, Inc.
175 Houston Street
San Antonio, Texas 78205

Cc: Lisa A. Martinelli, Vice President, Chief Privacy Officer, Highmark Health

EQUIFAX®

About the Equifax Credit Watch™ Gold identity theft protection product

Equifax Credit Watch will provide you with an "early warning system" to changes to your credit file. Note: You must be over age 18 with a credit file in order to take advantage of the product.

Equifax Credit Watch provides you with the following key features and benefits:

- Comprehensive credit file monitoring and automated alerts of key changes to your **Equifax** credit report
- Wireless alerts and customizable alerts available (available online only)
- Access to your Equifax Credit Report™
- Up to $25,000 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: You can sign up online or over the phone

To sign up online for **online delivery** go towww.myservices.equifax.com/gold

1. Welcome Page: Enter the Activation Code provided at the top of this page in the "Activation Code" box and click the "Submit" button.
2. Register: Complete the form with your contact information (name, gender, home address, date of birth, Social Security Number and telephone number) and click the "Continue" button.
3. Create Account: Complete the form with your email address, create a User Name and Password, check the box to accept the Terms of Use and click the "Continue" button.
4. Verify ID: The system will then ask you up to four security questions to verify your identity. Please answer the questions and click the "Submit Order" button.
5. Order Confirmation: This page shows you your completed enrollment. Please click the "View My Product" button to access the 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. Activation Code: You will be asked to enter your enrollment code as provided at the top of this 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 cannot 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 fraud alert on your credit file, visit: www.fraudalerts.equifax.com or you may contact the Equifax 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.

† Identity Theft Insurance underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions. This product is not intended for minors (under 18 years of age)

* The Automatic Fraud Alert feature made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC