

Return Mail Processing Center  
P.O. Box 6336  
Portland, OR 97228-6336

<<Mail ID>>  
<<Name 1>>  
<<Name 2>>  
<<Address 1>>  
<<Address 2>>  
<<Address 3>>  
<<Address 4>>  
<<Address 5>>  
<<City>><<State>><<Zip>>  
<<Country>>

<<Date>>

Re: Notice of Data Breach

Dear <<Name1>>:

Valley Presbyterian Hospital Foundation (“Valley Presbyterian”) writes to inform you of an incident that may affect the privacy of some of your information. On Thursday, July 31, 2020, Valley Presbyterian received notification from one of our third-party vendors, Blackbaud, Inc. (“Blackbaud”), of a cyber incident. Blackbaud is a cloud-computing provider that offers customer relationship management and financial services tools to organizations, including Valley Presbyterian. Upon receiving notice of the cyber incident, we immediately commenced an investigation to better understand the nature and scope of the incident and any impact on Valley Presbyterian data. This notice provides information about the Blackbaud incident, our response, and resources available to you to help protect your information from possible misuse, should you feel it necessary to do so.

**What Happened?** Blackbaud reported that it experienced a ransomware incident that resulted in encryption of certain Blackbaud systems between May 14, 2020 and May 20, 2020. Blackbaud advised it reported the incident to law enforcement and worked with forensic investigators to determine the nature and scope of the incident. Following its investigation, Blackbaud notified its customers that an unknown actor may have accessed or acquired certain Blackbaud customer data. Blackbaud reported that the data was exfiltrated by the threat actor at some point before Blackbaud locked the threat actor out of the environment on May 20, 2020. Upon learning of the Blackbaud incident, Valley Presbyterian immediately commenced an investigation to determine what, if any, sensitive Valley Presbyterian data was potentially involved. This investigation included working diligently to gather further information from Blackbaud to understand the scope of the incident, and on December 14, 2020, we determined the total population of affected individuals and their contact information.

**What Information was Involved?** Our investigation determined that the involved Blackbaud systems contained your name and <<Data Elements>>. Please note that, to date, we have not received confirmation from Blackbaud that your specific information was accessed or acquired by the unknown actor.

**What We Are Doing.** The confidentiality, privacy, and security of information in our care are among our highest priorities, and we take this incident very seriously. We will also be notifying state and federal regulators, as required. We are also providing, at no cost to you, complimentary credit monitoring through the services of TransUnion for twelve months. Please note that while we are making these services available to you, we are unable to enroll you in these services ourselves. Enrollment information is below:

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*myTrueIdentity*) for one year provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

To enroll in this service, go directly to the *myTrueIdentity* website at [www.mytrueidentity.com](http://www.mytrueidentity.com) and in the space referenced as “Enter Activation Code”, enter the following unique 12-letter Activation Code <<Activation Code>> and follow the three steps to receive your credit monitoring service online within minutes.

If you do not have access to the Internet and wish to enroll in a similar offline, paper based, credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the following 6-digit telephone pass code <<Passcode>> and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and <<Enrollment Deadline>>. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion, or an address in the United States (or its territories) and a valid Social Security number, or are under the age of 18. Enrolling in this service will not affect your credit score.

Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score. The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The service also includes access to an identity restoration program that provides assistance in the event your identity is compromised to help you restore your identity and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

***What You Can Do.*** We encourage you to review the enclosed *Steps You Can Take to Help Protect Your Information*. There you will find general information on what you can do to help protect your personal information.

We understand that you may have questions about the Blackbaud incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 818-902-2939 between the hours of 8am-4:30pm Pacific. You may also write to Valley Presbyterian at Attention: Privacy Officer, 15107 Vanowen St., Van Nuys, CA 91405.

We sincerely regret any inconvenience or concern this incident has caused.

Sincerely,

A handwritten signature in black ink, appearing to read "Lori Cardle". The signature is fluid and cursive, written in a professional style.

Lori Cardle  
Senior Vice President, Chief Operating Officer

## ***STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION***

### **Monitor Accounts**

In general, we encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a “security freeze” on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

#### **Experian**

P.O. Box 9554  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com/freeze/center.html](http://www.experian.com/freeze/center.html)

#### **TransUnion**

P.O. Box 160  
Woodlyn, PA 19094  
1-888-909-8872  
[www.transunion.com/credit-freeze](http://www.transunion.com/credit-freeze)

#### **Equifax**

P.O. Box 105788  
Atlanta, GA 30348-5788  
1-800-685-1111  
[www.equifax.com/personal/credit-report-services](http://www.equifax.com/personal/credit-report-services)

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five years, the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, military identification, etc.); and
7. If you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended “fraud alert” on your file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

#### **Experian**

P.O. Box 9554  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com/fraud/center.html](http://www.experian.com/fraud/center.html)

#### **TransUnion**

P.O. Box 2000  
Chester, PA 19016  
1-800-680-7289  
[www.transunion.com/fraud-victim-resource/place-fraud-alert](http://www.transunion.com/fraud-victim-resource/place-fraud-alert)

#### **Equifax**

P.O. Box 105069  
Atlanta, GA 30348  
1-888-766-0008  
[www.equifax.com/personal/credit-report-services](http://www.equifax.com/personal/credit-report-services)

### **Additional Information**

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; [www.identitytheft.gov](http://www.identitytheft.gov); 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General.

This investigation has not been delayed as a result of a law enforcement investigation.

**California Residents:** Visit the California Office of Privacy Protection ([www.oag.ca.gov/privacy](http://www.oag.ca.gov/privacy)) for additional information on protection against identity theft.