

RECEIVED

OCT 21 2020

CONSUMER PROTECTION

Yale
NewHaven
Health
Lawrence + Memorial
Hospital

VIA CERTIFIED MAIL
RETURN RECEIPT REQUESTED

October 15, 2020

Office of the Attorney General
33 Capitol Street
Concord, NH 03301

RE: Notification of Blackbaud, Inc. Security Breach

Dear Office of the Attorney General:

In accordance with N.H. Rev. Stat. Ann. § 359-C:20(I)(b), Lawrence + Memorial Hospital (“L+M”) is writing to notify the Office of the Attorney General (the “Office”) that 97 New Hampshire residents are being notified of a security breach that occurred at Blackbaud, Inc. (“Blackbaud”), a software company L + M has long used for donor communications and engagement. Blackbaud has a primary place of business at 65 Fairchild Street, Charleston, SC 29492, and L + M considers Mark Henly, who may be contacted at 1-843-716-3676, to be its primary contact at Blackbaud. Please note that no L + M system or service, and no data maintained by L + M, were involved in this security breach.

I. Brief Description of the Breach

This particular breach was part of a global security incident that affected many of Blackbaud’s 35,000 worldwide clients. On August 12, 2020, L + M was notified by Blackbaud that an unauthorized party had removed certain data as part of a ransomware attack on Blackbaud systems at some point between February 7 and May 20, 2020. Based upon our investigation of the incident, we have determined that the following types of personal information were involved in the incident: full name, address, phone number, date of birth, philanthropic history, names of health care providers, and dates of service. With respect to one of the 97 impacted individuals, the data also included credit card information.

II. Response to the Breach

Blackbaud informed L + M that, upon discovery of the ransomware event, Blackbaud, together with independent forensics experts and law enforcement, successfully stopped the cybercriminal from blocking its system and fully encrypting files. However, despite these actions, the cybercriminal was able to remove a copy of a subset of data from Blackbaud’s self-hosted

environment. Blackbaud further assured L + M that Blackbaud had made a payment in response to a demand from the cybercriminal and any stolen data has been destroyed. Blackbaud also does not believe the data has been disseminated in any manner. However, L + M is not able to independently validate these assurances.

L + M has worked diligently to identify the patients and donors whose information was contained in the Blackbaud systems, which include certain New Hampshire residents. Although L + M is not aware of any fraud or identity theft to any individual as a result of this incident, L + M is notifying the potentially impacted New Hampshire residents in accordance with applicable law. A template copy of each form of the notification that was sent to impacted individuals on October 13, 2020 is attached. L + M is offering the one New Hampshire resident whose credit card information was included within the data a complimentary one-year membership of Experian IdentityWorks Credit 3B.

I want to assure you that L + M expects its vendors to adhere to the highest of privacy standards. If you have any questions, you may contact me at the information listed below

Sincerely,



Marc C. Lombardi
Deputy General Counsel
Yale New Haven Health

789 Howard Ave., CB230
New Haven, CT 06519
marc.lombardi@ynhh.org
203.688.1335

Yale
NewHaven
Health

Lawrence + Memorial
Hospital

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

On behalf of Lawrence + Memorial Hospital, we are writing to make you aware of a recent data security incident at Blackbaud, a software company the hospital has long used for donor communications and engagement. Lawrence + Memorial Hospital is one of a large number of organizations affected by this incident. While your personal financial information such as bank account, Social Security numbers or credit card information was not involved in this incident, we wanted you to be aware of the incident as a measure of full transparency.

Unfortunately, the occurrence and sophistication of cybercrimes has increased significantly in recent years. This particular breach was part of a global security incident that affected many of Blackbaud's 35,000 worldwide clients. We were notified by Blackbaud on August 14, 2020, that an unauthorized party had removed non-financial information as part of a ransomware attack on Blackbaud systems at some point between February 7 and May 20, 2020. However, we were assured that Blackbaud made a payment in response to a demand from the outside party and the matter was addressed.

We now understand that certain demographic information such as names, addresses, phone numbers, dates of birth and philanthropic history were included in the Blackbaud databases subject to the incident. Additionally, there may have been information related to the name of your doctor or dates of service at our hospital. Please understand that the cyber attackers never, at any time, had access to our electronic medical record system.

Blackbaud has assured its clients that any stolen data has been destroyed and they do not believe it has been disseminated in any manner. However, we are not able to independently validate that assurance.

Lawrence + Memorial Hospital understands that your privacy is critically important and we truly value the relationship with our community and the trust you put in us as a community resource. We take the security of your information very seriously. We will continue to work with the vendor to ensure that your data are well protected. In the meantime, we are reviewing our relationship with Blackbaud. We recommend that you stay aware of any unusual activity, including any solicitations for unknown charities.

On behalf of Lawrence + Memorial Hospital, we apologize for this incident and truly regret any inconvenience this has caused. It is our goal as a premier healthcare provider to demonstrate respect for patients and our community and to always safeguard your information. If you have any questions regarding this incident and your information, please call 1-888-479-3575, Monday through Friday, between 9:00 a.m. and 6:30 p.m. Eastern Time. You can access additional information related to the Blackbaud breach on this site: <https://www.blackbaud.com/securityincident>.

Sincerely,



Patrick L. Green, FACHE
President & CEO
Lawrence + Memorial Hospital and
Westerly Hospital
Executive Vice President, Yale New Haven Health



Christine M. Meola
Vice President
Office of Development
Lawrence + Memorial Hospital
Westerly Hospital

Yale
NewHaven
Health

Lawrence + Memorial
Hospital

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

On behalf of Lawrence + Memorial Hospital, we are writing to make you aware of a recent data security incident at Blackbaud, a software company the hospital has long used for donor communications and engagement. Lawrence + Memorial Hospital is one of a large number of organizations affected by this incident.

Unfortunately, the occurrence and sophistication of cybercrimes has increased significantly in recent years. This particular breach was part of a global security incident that affected many of Blackbaud's 35,000 worldwide clients. We were notified by Blackbaud on August 12, 2020, that an unauthorized party had removed non-financial information as part of a ransomware attack on Blackbaud systems at some point between February 7 and May 20, 2020. However, we were assured that Blackbaud made a payment in response to a demand from the outside party and the matter was addressed.

We now understand that certain demographic information such as names, addresses, phone numbers, dates of birth and philanthropic history were included in the Blackbaud databases subject to the incident. There may have been information related to the name of your doctor or dates of service at our hospital. Additionally, we found that some of your financial information, including credit card information, was within the data. Please understand that the cyber attackers never, at any time, had access to our electronic medical record system.

Blackbaud has assured its clients that any stolen data has been destroyed and they do not believe it has been disseminated in any manner. However, we are not able to independently validate that assurance.

Lawrence + Memorial Hospital understands that your privacy is critically important and we truly value the relationship with our community and the trust you put in us as a community resource. We take the security of your information very seriously. We will continue to work with the vendor to ensure that your data are protected. In the meantime, we are reviewing our relationship with Blackbaud. We recommend that you stay aware of any unusual activity, including any solicitations for unknown charities.

Out of an abundance of caution, we are offering a complimentary one-year membership of Experian IdentityWorksSM Credit 3B. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. IdentityWorks Credit 3B is completely free to you and enrolling in this program will not hurt your credit score. For more information on identity theft prevention and IdentityWorks Credit 3B, including instructions on how to activate your complimentary one-year membership, please see the additional information provided in this below.

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: <<b2b_text_1(EnrollmentDeadline)>> (Your code will not work after this date.)
2. VISIT the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
3. PROVIDE the Activation Code: <<Member ID>>

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-288-8057. Be prepared to provide engagement number <<b2b_text_2(EngagementNumber)>> as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

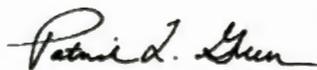
- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Activate your membership today at <https://www.experianidworks.com/3bcredit> or call 877-288-8057 to register with the activation code above.

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-288-8057.

On behalf of Lawrence + Memorial Hospital, we apologize for this incident and truly regret any inconvenience this has caused. It is our goal as a premier healthcare provider to demonstrate respect for patients and our community and to always safeguard your information. If you have any questions regarding this incident and your information, please call 1-888-479-3575, Monday through Friday, between 9:00 a.m. and 6:30 p.m. Eastern Time. You can access additional information related to the Blackbaud breach on this site: <https://www.blackbaud.com/securityincident>.

Sincerely,



Patrick L. Green, FACHE
President & CEO
Lawrence + Memorial Hospital and
Westerly Hospital
Executive Vice President, Yale New Haven Health



Christine M. Meola
Vice President
Office of Development
Lawrence + Memorial Hospital
Westerly Hospital

Additional Information

You should regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax: P.O. Box 740241, Atlanta, Georgia 30374-0241, 1-800-685-1111, www.equifax.com

Experian: P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com

TransUnion: P.O. Box 1000, Chester, PA 19022, 1-800-888-4213, www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts, creditor inquiries, or medical bills that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding identity theft. The FTC can be contacted using the following information:

Federal Trade Commission, Consumer Response Center

600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

You should regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive regular explanation of benefits statements, contact your provider and request them to send such statements following the provision of services in your name or number.

Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider, to serve as a baseline.

We will not email or call you regarding this event: Please be aware that we will not email or call you regarding this event, nor will we, or anyone acting on our behalf, email or call you to request your social security number, credit card information, or any other personal information from you with regard to this event. If you receive any emails or calls regarding this event, which request any such information, please do not respond or provide any such information.

Fraud Alerts: You may also call the toll-free number of any of the three nationwide consumer reporting companies to place an initial fraud alert on your credit reports. There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one (1) year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three national credit reporting agencies listed below.

Equifax: 1-888-766-0008, www.equifax.com

Experian: 1-888-397-3742, www.experian.com

TransUnion: 1-800-680-7289, fraud.transunion.com

Credit Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze, free of charge. The FTC's website, at <http://www.consumer.ftc.gov/articles/0279-extended-fraud-alerts-and-credit-freezes>, explains some of the basics of a "credit freeze" and how it differs from an initial fraud alert. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.

Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax: P.O. Box 105788, Atlanta, GA 30348, www.equifax.com

Experian: P.O. Box 9554, Allen, TX 75013, www.experian.com

TransUnion LLC: P.O. Box 2000, Chester, PA, 19022-2000, freeze.transunion.com

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.