



MULLEN
COUGHLIN_{LLC}
ATTORNEYS AT LAW

Michael J. Bonner
Office: (267) 930-4815
Fax: (267) 930-4771
Email: mbonner@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

September 3, 2020

VIA U.S. MAIL

Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Sir or Madam:

We represent Samaritan Healthcare & Hospice (“Samaritan”), located at 3906 Church Road, Mount Laurel, NJ 08054, and are writing to notify your Office of an incident that may affect the security of some personal information relating to one (1) New Hampshire resident. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Samaritan does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On July 16, 2020, Blackbaud, Inc. (“Blackbaud”), reported to Samaritan that in May 2020, Blackbaud experienced a ransomware incident that resulted in encryption of certain Blackbaud systems. Blackbaud reported the incident to law enforcement and worked with forensic investigators to investigate. Following its investigation, Blackbaud notified Samaritan that an unknown actor may have accessed or acquired certain Blackbaud customer data. Blackbaud reported that data was removed by the unknown actor at some point before Blackbaud locked the unknown actor out of their systems on May 20, 2020.

Upon learning of the Blackbaud incident, Samaritan immediately moved to determine what, if any, personal information was potentially involved. This investigation included working diligently to gather additional information from Blackbaud to understand the scope of the incident. On August

2020 SEP -8 PM 1:07
OFFICE OF THE ATTORNEY GENERAL

6, 2020, Samaritan determined the information potentially affected by Blackbaud's incident may have contained personal information. The information potentially impacted by this incident includes name, address, and driver's license number.

Notice to New Hampshire Resident

On September 3, 2020, Samaritan began providing written notice of this incident to affected individuals, which includes one (1) New Hampshire resident. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit A*.

Other Steps Taken and To Be Taken

Upon discovering the event, Samaritan moved quickly to investigate and respond to the incident, including requesting additional information from Blackbaud to identify potentially impacted individuals. Samaritan is reviewing its existing policies and procedures regarding third-party vendors and working with Blackbaud to confirm the use of additional measures and safeguards to protect against this type of incident in the future.

Samaritan is providing access to credit monitoring services for twelve (12) months, through Transunion, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals. Additionally, Samaritan is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Samaritan is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4815.

Very truly yours,



Michael J. Bonner of
MULLEN COUGHLIN LLC

EXHIBIT A

Samaritan

LIFE-ENHANCING CARE

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

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

<<Date>>

Dear <<Name 1>>:

Samaritan is incredibly grateful for you and all our volunteers, and so I am regrettably writing to notify you of an incident impacting one of our vendors that may affect the privacy of some of your information. The vendor is Blackbaud, and Samaritan uses the Blackbaud software system to manage information required to coordinate our volunteer services. Blackbaud is a cloud computing company that offers customer relationship management and financial services tools to Samaritan and other organizations. We take this incident very seriously and want to provide you with information about the incident along with access to resources so that you can better protect your information should you feel it necessary to do so.

What Happened: On July 16, 2020, Blackbaud reported to us that in May 2020, they had experienced a ransomware incident that resulted in encryption of certain Blackbaud systems. Blackbaud reported the incident to law enforcement and worked with forensic investigators to investigate. Following its investigation, Blackbaud notified Samaritan and its other customers that an unknown actor may have accessed or acquired certain Blackbaud customer data. Blackbaud reported that data was removed by the unknown actor at some point before Blackbaud locked the unknown actor out of their systems on May 20, 2020.

Upon learning of the Blackbaud incident, Samaritan immediately moved to determine what, if any, sensitive information was potentially involved. This investigation included working diligently to gather additional information from Blackbaud to understand the scope of the incident. On or about August 6, 2020, Samaritan determined the information potentially affected may have contained personal information.

What Information Was Involved: Our investigation determined that the Blackbaud systems contained your name and <<Data Elements>>. Please note that, to date, we have not received any information from Blackbaud indicating that your information was specifically 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. As part of our ongoing commitment to the security of information in our care, we are reviewing our existing policies and procedures regarding our third-party vendors. We are also working with Blackbaud to confirm their use of additional measures and safeguards to protect against this type of incident in the future. We will also be notifying government regulators, as required.

Resources Available to You: Samaritan is providing information to help you protect against identity theft and fraud, as well as access to 12 months of credit monitoring and identity protection services with Transunion at no cost to you. Because the enrollment process does not allow us to enroll you on your behalf, you will need to enroll yourself by following the enclosed instructions.

What You Can Do: Please review the enclosed “Steps You Can Take to Protect Your Information” to learn more about ways to safeguard your personal information. You may also enroll in the free credit monitoring and identity protection services offered by Samaritan.

For More Information: We understand that you may have questions about credit protection services we are offering and encourage you to contact our dedicated assistance line at 855-907-2141 Monday through Friday 9am to 9pm Eastern Time.

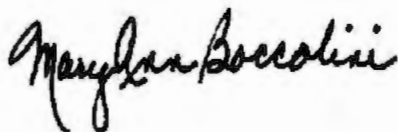
For any additional questions, please contact one of my colleagues noted below during regular business hours. You may also write to Samaritan at 3906 Church Road, Mount Laurel, New Jersey 08054.

Chris Rollins
Chief Development Officer
856-552-3287
CRollins@samaritanNJ.org

Joanne Rosen
VP, Marketing & Public Affairs
856-552-3254
JRosen@samaritanNJ.org

We truly regret any inconvenience this may cause. We truly value and appreciate our relationship with you and all our volunteers. We thank you for your service to Samaritan and your support for our commitment to providing life-enhancing care for our patients and their families.

Sincerely,



Mary Ann Boccolini
President/Chief Executive Officer



Activation Code: <<Activation Code>>

Enroll in Credit Monitoring

Complimentary One-Year *myTrueIdentity* 3B Credit Monitoring Service

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

How to Enroll: You can sign up online or via U.S. mail delivery

- To enroll in this service, go to the *myTrueIdentity* website at www.MyTrueIdentity.com and, in the space referenced as "Enter Activation Code," enter the 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, three-bureau 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 six-digit telephone passcode <<Pass Code>> 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 <<Deadline to Enroll>>. 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. Enrolling in this service will not affect your credit score.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH COMPLIMENTARY CREDIT MONITORING SERVICE:

- 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 three-bureau credit monitoring service will notify you if there are any critical changes to your credit files at TransUnion,[®] Experian,[®] and Equifax,[®] including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more.
- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

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 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 that 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

TransUnion
P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872

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

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 (5) years, provide 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.);
7. If you are a victim of identity theft, include 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 1-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

TransUnion
P.O. Box 2000
Chester, PA 19016
1-800-680-7289

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

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, 1-877-ID-THEFT (1-877-438-4338); 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.

For North Carolina residents, the Attorney General can be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6400; or www.ncdoj.gov.

For Maryland residents, the Attorney General can be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662; or www.oag.state.md.us. Samaritan may be contacted by mail at 3906 Church Road, Mount Laurel, NJ 08054.

For New York residents, the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.