



MULLEN  
COUGHLIN<sup>LLC</sup>  
ATTORNEYS AT LAW

Sian M. Schafle  
Office: (267) 930-4799  
Fax: (267) 930-4771  
Email: [sschafle@mullen.law](mailto:sschafle@mullen.law)

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

September 18, 2020

**VIA E-MAIL**

Office of the Attorney General  
1125 Washington Street SE  
PO Box 40100  
Olympia, WA 98504-0100  
E-mail: [securitybreach@atg.wa.gov](mailto:securitybreach@atg.wa.gov)

**Re: Notice of Data Event**

Dear Sir or Madam:

We represent Joslin Diabetes Center (“Joslin”) located at One Joslin Place, 4th Floor, Boston, MA 02215, and are writing to notify your office of an incident that may affect the security of some personal information relating to one-thousand two hundred twelve (1,212) Washington residents. Joslin reserves the right to supplement this notice with any new significant facts learned subsequent to its submission. By providing this notice, Joslin does not waive any rights or defenses regarding the applicability of Washington law, the applicability of the Washington data event notification statute, or personal jurisdiction.

**Nature of the Data Event**

On July 16, 2020, Joslin received notification from one of its third-party vendors, Blackbaud, Inc. (“Blackbaud”), of a cyber incident. Blackbaud reported that, in May 2020, it experienced a ransomware incident that resulted in encryption of certain Blackbaud systems. Blackbaud advised that it reported the incident to law enforcement and worked with forensic investigators to determine the nature and scope of the incident. Following its investigation, and two months after the incident, Blackbaud notified its customers, including Joslin, that an unknown actor may have accessed or acquired certain Blackbaud customer data at some point before Blackbaud locked the threat actor out of its environment on May 20, 2020. According to Blackbaud, it detected the first indicator of compromise on May 14, 2020 and that unauthorized activity was contained and stopped by May 20, 2020.

Upon learning of the Blackbaud incident, Joslin immediately commenced an investigation to determine what, if any, sensitive Joslin data was potentially involved. On or about August 5, 2020, Joslin received additional information from Blackbaud on the incident. Because Blackbaud failed to provide a list of the potentially affected Joslin data Joslin undertook a comprehensive analysis of the information Blackbaud provided and the data stored on the systems identified by Blackbaud to confirm what records could have

been accessible to the threat actor and to identify the individuals associated with the records. On or about August 20, 2020, Joslin completed its investigation and confirmed that personal information as defined by Wash. Rev. Code Ann. § 19.255.005 could have been subject to unauthorized access or acquisition including name, date of birth, and medical information including treating physician and date and location of treatment.

### **Notice to Washington Residents**

On September 18, 2020, Joslin will provide written notice of the Blackbaud incident to one-thousand two hundred twelve (1,212) Washington residents. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit A*. Joslin also posted notice of the Blackbaud incident on its website and issued a nationwide media notice on September 14, 2020. To date, Joslin has not received any information from Blackbaud that any Joslin information was specifically accessed or acquired by the unknown actor.

### **Other Steps Taken and To Be Taken**

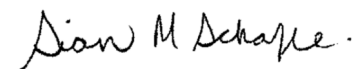
Upon discovering the event, Joslin moved quickly to obtain information from Blackbaud regarding their incident. Joslin then provided notice to potentially affected individuals associated with Joslin. That notice provided information about the Blackbaud incident, Joslin's response thereto, and resources available to help protect personal information from possible misuse. Joslin's response included extensive attempts to coordinate with Blackbaud to confirm what information could have been potentially affected that may have contained personal information. Joslin is working to review existing policies and procedures regarding third-party vendors and is working with Blackbaud to evaluate additional measures and safeguards to protect against this type of incident in the future.

Additionally, Joslin is providing notified individuals with a toll-free dedicated call center to ask further questions, guidance on how to better protect against identity theft and fraud. Joslin is providing individuals with 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. Joslin has notified the United States Department of Health and Human Services, Office of Civil Rights and will be notifying state regulators as required.

### **Contact Information**

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4799.

Very truly yours,



Sian M. Schafle of  
MULLEN COUGHLIN LLC

# Exhibit A

<<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>>,

Joslin Diabetes Center (“Joslin”) writes to inform you of a recent incident involving Blackbaud, Inc. (“Blackbaud”), a third-party vendor that Joslin uses for database assistance in donor relations and fundraising operations. On July 16, 2020, Joslin received notification from Blackbaud of a cyber incident that Blackbaud uncovered in May 2020. The confidentiality, privacy, and security of information in our care are among our highest priorities, and we take this incident very seriously.

Upon receiving notice of the cyber incident, Joslin immediately began an investigation to better understand the nature and scope of the incident and any impact on Joslin’s 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.

Blackbaud reported that, in May 2020, two months before notifying Joslin, it discovered a ransomware incident that resulted in encryption of certain Blackbaud systems. Blackbaud reported the incident to law enforcement and worked with forensic investigators to determine the nature and scope of the incident. Blackbaud notified its customers, including Joslin, that a cybercriminal may have accessed or acquired certain Blackbaud customer data. Blackbaud reported that the data was potentially exported by the threat actor before Blackbaud locked the cybercriminal out of its environment on May 20, 2020. According to Blackbaud the data was destroyed and they do not believe that any data was or will be misused, disseminated or otherwise be made publicly available. Blackbaud further stated that this belief has been corroborated by outside experts and law enforcement.

Joslin has worked diligently to gather further information from Blackbaud to understand the incident. Our investigation determined that the involved Blackbaud systems may have contained your name, date of birth, treatment date, treatment location and physician name. We have not received any information from Blackbaud that your information was specifically accessed or acquired by the cybercriminal. It is important to note the Joslin data hosted by Blackbaud did not include any financial account information or social security numbers.

Your private information and its security are of the utmost importance to Joslin. We are reviewing our existing policies and procedures regarding our third-party vendors, and are working with Blackbaud to evaluate additional measures and safeguards to protect against this type of incident in the future.

While we have no reason to believe there are any specific actions you need to take in this situation, 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 888-977-0627 between the hours of 9:00 AM to 6:30 PM Eastern Time, Monday through Friday (may exclude certain U.S. holidays). You may also write to Joslin at:

Joslin Diabetes Center  
One Joslin Place, Suite 401  
Boston, MA 02215  
Attention: Privacy Officer

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

Sincerely,

Joslin Diabetes Center

## **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.

The major credit reporting agencies are listed below:

#### **Experian**

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

#### **TransUnion**

P.O. Box 2000  
Chester, PA 19016  
1-888-909-8872  
[www.transunion.com](http://www.transunion.com)

#### **Equifax**

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

### **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); 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 Maryland residents**, the Attorney General can be contacted at 200 St. Paul Place, 16<sup>th</sup> Floor, Baltimore, MD 21202, 1-410-528-8662; 1-888-743-0023; or [www.oag.state.md.us](http://www.oag.state.md.us).

**For Rhode Island residents**, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, Rhode Island 02903; [www.riag.ri.gov](http://www.riag.ri.gov); or 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. [There are approximately 1,453 Rhode Island residents whose information may have been present.](#)

**For Washington, D.C. residents**, the Office of Attorney General for the District of Columbia can be reached at: 441 4<sup>th</sup> Street NW, Suite 1100 South, Washington, D.C. 20001; 1-202-442-9828; <https://oag.dc.gov>.

<<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>>,

Joslin Diabetes Center (“Joslin”) writes to inform you of a recent incident involving Blackbaud, Inc. (“Blackbaud”), a third-party vendor that Joslin uses for database assistance in donor relations and fundraising operations. On July 16, 2020, Joslin received notification from Blackbaud of a cyber incident that Blackbaud uncovered in May 2020. The confidentiality, privacy, and security of information in our care are among our highest priorities, and we take this incident very seriously.

Upon receiving notice of the cyber incident, Joslin immediately began an investigation to better understand the nature and scope of the incident and any impact on Joslin’s 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.

Blackbaud reported that, in May 2020, two months before notifying Joslin, it discovered a ransomware incident that resulted in encryption of certain Blackbaud systems. Blackbaud reported the incident to law enforcement and worked with forensic investigators to determine the nature and scope of the incident. Blackbaud notified its customers, including Joslin, that a cybercriminal may have accessed or acquired certain Blackbaud customer data. Blackbaud reported that the data was potentially exported by the threat actor before Blackbaud locked the cybercriminal out of its environment on May 20, 2020. According to Blackbaud the data was destroyed and they do not believe that any data was or will be misused, disseminated or otherwise be made publicly available. Blackbaud further stated that this belief has been corroborated by outside experts and law enforcement.

Joslin has worked diligently to gather further information from Blackbaud to understand the incident. Our investigation determined that the involved Blackbaud systems may have contained your name and date of birth. We have not received any information from Blackbaud that your information was specifically accessed or acquired by the cybercriminal. It is important to note the Joslin data hosted by Blackbaud did not include any financial account information or social security numbers.

Your private information and its security are of the utmost importance to Joslin. We are reviewing our existing policies and procedures regarding our third-party vendors, and are working with Blackbaud to evaluate additional measures and safeguards to protect against this type of incident in the future.

While we have no reason to believe there are any specific actions you need to take in this situation, 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 888-977-0627 between the hours of 9:00 AM to 6:30 PM Eastern Time, Monday through Friday (may exclude certain U.S. holidays). You may also write to Joslin at:

Joslin Diabetes Center  
One Joslin Place, Suite 401  
Boston, MA 02215  
Attention: Privacy Officer

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

Sincerely,

Joslin Diabetes Center

## ***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.

The major credit reporting agencies are listed below:

#### **Experian**

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

#### **TransUnion**

P.O. Box 2000  
Chester, PA 19016  
1-888-909-8872  
[www.transunion.com](http://www.transunion.com)

#### **Equifax**

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

### **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); 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.