ARCHER
THE ARCHER SCHOOL FOR GIRLS

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

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

Re: Notice of Data Breach

Dear <<first_name>>:

The Archer School for Girls ("Archer") is writing to notify you of a data security incident that occurred at one of our vendors, Blackbaud, Inc. ("Blackbaud"). This notice explains the incident and measures taken in response.

What Happened?

Blackbaud is a cloud-based software company that provides services to thousands of schools, hospitals, and other non-profits, including Archer. On July 16, 2020, Blackbaud notified us and many other institutions that it had discovered an attempted encryption attack on Blackbaud's network in May 2020. Blackbaud reported that it conducted an investigation, determined that backup files containing information from its clients had been taken from its network, and an attempt was made to encrypt files to convince Blackbaud to pay a ransom. Blackbaud paid the ransom and obtained confirmation that the files that had been removed by the unauthorized individual had been destroyed. The time period of unauthorized access was between February 7, 2020, and May 20, 2020. Blackbaud also reported that it has been working with law enforcement.

Upon learning of the incident from Blackbaud, we conducted our own investigation to determine what information was involved in the Blackbaud incident. Initially, Blackbaud informed us that the fields in the database backups containing personal information were encrypted and therefore not accessible by the unauthorized individual. However, Blackbaud's further investigation determined that was not the case, and informed us of its updated findings on September 29, 2020. We worked with Blackbaud to identify the individuals whose information may have been involved and determined on November 10, 2020, that the backup files contained certain unencrypted information pertaining to you.

What Information Was Involved?

The backup file involved contained your **<<b2b_text_1(Impacted Data)>>**. Blackbaud has assured us that the backup file has been destroyed by the unauthorized individual and there is no reason to believe any data was or will be misused, disseminated, or otherwise be made available publicly.

What You Can Do.

While we have no evidence that your personal information has been misused, we wanted to let you know this happened and assure you we take it very seriously. As a precaution, Blackbaud is offering you a complimentary membership to Identity Monitoring and Fraud Resolution services for two years. This product provides you with identity detection and resolution of identity theft. These services are completely free to you and enrolling in this program will not hurt your credit score. If your health insurance or medical information was involved, it is also advisable to review the billing statements you receive from your health insurer or healthcare provider. If you see charges for services you did not receive, please contact the insurer or provider immediately.

For more information on further steps you can take in response, including enrolling in the free Identity Monitoring and Fraud Resolution services being offered to you, please see the additional information provided in the following pages.

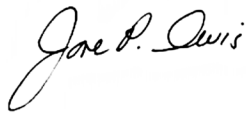
What We Are Doing.

We are notifying you of this incident and sharing the steps that we and Blackbaud are taking in response. Blackbaud has informed us that it identified and fixed the vulnerability associated with this incident, implemented several changes that will better protect your data from any subsequent incidents, and is undertaking additional efforts to harden its environment through enhancements to access management, network segmentation, and deployment of additional endpoint and network-based monitoring tools.

For More Information:

We regret that this occurred and apologize for any inconvenience. Should you have any further questions or concerns regarding this matter, please do not hesitate to contact our dedicated helpline at <<1-XXX-XXX-XXXX>>, Monday through Friday, from 8:00 a.m. to 5:30 p.m. Central Time.

Sincerely,



Jane P. Davis
Chief Financial Officer | The Archer School for Girls

Information About Identity Monitoring and Fraud Resolution Services

How do I enroll for the free services?

To enroll in Credit Monitoring services at no charge, please navigate to:

[redacted]

If prompted, please provide the following unique code to gain access to services: [redacted]

Once registered, you can access Monitoring Services by selecting the "Use Now" link to fully authenticate your identity and activate your services. **Please ensure you take this step to receive your alerts.**

In order for you to receive the monitoring services described above, you must enroll by **March 27, 2021**.

Additional Information about Identity Monitoring and Fraud Resolution Services

We are providing you with access to **Single Bureau Credit Monitoring** services at no charge. Services are for 24 months from the date of enrollment. When changes occur to your Experian credit file, notification is sent to you the same day the change or update takes place with the bureau. In addition, we are providing you with proactive fraud assistance to help with any questions you might have. In the event you become a victim of fraud you will also have access remediation support from a CyberScout Fraud Investigator. In order for you to receive the monitoring service described above, you must enroll by **March 27, 2021**.

Proactive Fraud Assistance. For sensitive breaches focused on customer retention, reputation management, or escalation handling, CyberScout provides unlimited access during the service period to a fraud specialist who will work with enrolled notification recipients on a one-on-one basis, answering any questions or concerns that they may have. Proactive Fraud Assistance includes the following features:

- Fraud specialist-assisted placement of fraud alert, protective registration, or geographical equivalent, in situations where it is warranted.
- After placement of a Fraud Alert, a credit report from each of the three (3) credit bureaus is made available to the notification recipient (United States only).
- Assistance with reading and interpreting credit reports for any possible fraud indicators.
- Removal from credit bureau marketing lists while Fraud Alert is active (United States only).
- Answering any questions individuals may have about fraud.
- Provide individuals with the ability to receive electronic education and alerts through email. (Note that these emails may not be specific to the recipient's jurisdiction/location.)

Identity Theft and Fraud Resolution Services. Resolution services are provided for enrolled notification recipients who fall victim to an identity theft as a result of the applicable breach incident. ID Theft and Fraud Resolution includes, but is not limited to, the following features:

- Unlimited access during the service period to a personal fraud specialist via a toll-free number.
- Creation of Fraud Victim affidavit or geographical equivalent, where applicable.
- Preparation of all documents needed for credit grantor notification, and fraud information removal purposes.
- All phone calls needed for credit grantor notification, and fraud information removal purposes.
- Notification to any relevant government and private agencies.
- Assistance with filing a law enforcement report.
- Comprehensive case file creation for insurance and law enforcement.
- Assistance with enrollment in applicable Identity Theft Passport Programs in states where it is available and in situations where it is warranted (United States only).
- Assistance with placement of credit file freezes in states where it is available and in situations where it is warranted (United States only); this is limited to online-based credit freeze assistance.
- Customer service support for individuals when enrolling in monitoring products, if applicable.
- Assistance with review of credit reports for possible fraudulent activity.
- Unlimited access to educational fraud information and threat alerts. (Note that these emails may not be specific to the recipient's jurisdiction/location.)

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

Experian, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

ARCHER
THE ARCHER SCHOOL FOR GIRLS

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

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

Re: Notice of Data Breach

Dear <<first_name>>:

The Archer School for Girls ("Archer") is writing to notify you of a data security incident that occurred at one of our vendors, Blackbaud, Inc. ("Blackbaud"). This notice explains the incident and measures taken in response.

What Happened?

Blackbaud is a cloud-based software company that provides services to thousands of schools, hospitals, and other non-profits, including Archer. On July 16, 2020, Blackbaud notified us and many other institutions that it had discovered an attempted encryption attack on Blackbaud's network in May 2020. Blackbaud reported that it conducted an investigation, determined that backup files containing information from its clients had been taken from its network, and an attempt was made to encrypt files to convince Blackbaud to pay a ransom. Blackbaud paid the ransom and obtained confirmation that the files that had been removed by the unauthorized individual had been destroyed. The time period of unauthorized access was between February 7, 2020, and May 20, 2020. Blackbaud also reported that it has been working with law enforcement.

Upon learning of the incident from Blackbaud, we conducted our own investigation to determine what information was involved in the Blackbaud incident. Initially, Blackbaud informed us that the fields in the database backups containing personal information were encrypted and therefore not accessible by the unauthorized individual. However, Blackbaud's further investigation determined that was not the case, and informed us of its updated findings on September 29, 2020. We worked with Blackbaud to identify the individuals whose information may have been involved and determined on November 10, 2020, that the backup files contained certain unencrypted information pertaining to you.

What Information Was Involved?

The backup file involved contained your **<<b2b_text_1(Impacted Data)>>**. Blackbaud has assured us that the backup file has been destroyed by the unauthorized individual and there is no reason to believe any data was or will be misused, disseminated, or otherwise be made available publicly.

What You Can Do.

While we have no evidence that your personal information has been misused, we wanted to let you know this happened and assure you we take it very seriously. If your health insurance or medical information was involved, it is also advisable to review the billing statements you receive from your health insurer or healthcare provider. If you see charges for services you did not receive, please contact the insurer or provider immediately. For more information on further steps you can take in response, please see the additional information provided in the following pages.

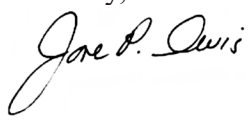
What We Are Doing.

We are notifying you of this incident and sharing the steps that we and Blackbaud are taking in response. Blackbaud has informed us that it identified and fixed the vulnerability associated with this incident, implemented several changes that will better protect your data from any subsequent incidents, and is undertaking additional efforts to harden its environment through enhancements to access management, network segmentation, and deployment of additional endpoint and network-based monitoring tools.

For More Information:

We regret that this occurred and apologize for any inconvenience. Should you have any further questions or concerns regarding this matter, please do not hesitate to contact our dedicated helpline at <<1-XXX-XXX-XXXX>>, Monday through Friday, from 8:00 a.m. to 5:30 p.m. Central Time.

Sincerely,



Jane P. Davis
Chief Financial Officer | The Archer School for Girls

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

Experian, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

ARCHER
THE ARCHER SCHOOL FOR GIRLS

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

To the Parent or Guardian of:
<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Re: Notice of Data Breach

Dear Parent or Guardian of <<first_name>>:

The Archer School for Girls ("Archer") is writing to notify you of a data security incident that occurred at one of our vendors, Blackbaud, Inc. ("Blackbaud"). This notice explains the incident and measures taken in response.

What Happened?

Blackbaud is a cloud-based software company that provides services to thousands of schools, hospitals, and other non-profits, including Archer. On July 16, 2020, Blackbaud notified us and many other institutions that it had discovered an attempted encryption attack on Blackbaud's network in May 2020. Blackbaud reported that it conducted an investigation, determined that backup files containing information from its clients had been taken from its network, and an attempt was made to encrypt files to convince Blackbaud to pay a ransom. Blackbaud paid the ransom and obtained confirmation that the files that had been removed by the unauthorized individual had been destroyed. The time period of unauthorized access was between February 7, 2020, and May 20, 2020. Blackbaud also reported that it has been working with law enforcement.

Upon learning of the incident from Blackbaud, we conducted our own investigation to determine what information was involved in the Blackbaud incident. Initially, Blackbaud informed us that the fields in the database backups containing personal information were encrypted and therefore not accessible by the unauthorized individual. However, Blackbaud's further investigation determined that was not the case, and informed us of its updated findings on September 29, 2020. We worked with Blackbaud to identify the individuals whose information may have been involved and determined on November 10, 2020, that the backup files contained certain unencrypted information pertaining to your child.

What Information Was Involved?

The backup file involved contained your child's **<<b2b_text_1(Impacted Data)>>**. Blackbaud has assured us that the backup file has been destroyed by the unauthorized individual and there is no reason to believe any data was or will be misused, disseminated, or otherwise be made available publicly.

What You Can Do.

While we have no evidence that your child's personal information has been misused, we wanted to let you know this happened and assure you we take it very seriously. If your child's health insurance or medical information was involved, it is also advisable to review the billing statements you receive from your child's health insurer or healthcare provider. If you see charges for services your child did not receive, please contact the insurer or provider immediately. For more information on further steps you can take in response, please see the additional information provided in the following pages.

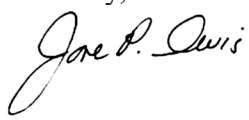
What We Are Doing.

We are notifying you of this incident and sharing the steps that we and Blackbaud are taking in response. Blackbaud has informed us that it identified and fixed the vulnerability associated with this incident, implemented several changes that will better protect data from any subsequent incidents, and is undertaking additional efforts to harden its environment through enhancements to access management, network segmentation, and deployment of additional endpoint and network-based monitoring tools.

For More Information:

We regret that this occurred and apologize for any inconvenience. Should you have any further questions or concerns regarding this matter, please do not hesitate to contact our dedicated helpline at <<1-XXX-XXX-XXXX>>, Monday through Friday, from 8:00 a.m. to 5:30 p.m. Central Time.

Sincerely,



Jane P. Davis
Chief Financial Officer | The Archer School for Girls

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your child's account statements and free credit reports for any unauthorized activity. Parents or guardians may request a copy of their child's or ward's credit information by contacting the three credit bureaus. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe your child is the victim of identity theft or have reason to believe your child's personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your child's records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

Fraud Alerts: There are two types of fraud alerts you can place on your child's credit report to put your child's creditors on notice that your child 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 child's credit report if you suspect your child has been, or is about to be, a victim of identity theft. An initial fraud alert stays on your child's credit report for one year. You may have an extended alert placed on your child's credit report if your child has already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your child's credit report for seven years. You can place a fraud alert on your child's credit report by contacting any of the three national credit reporting agencies.

Credit Freezes: You have the right to put a credit freeze, also known as a security freeze, on your child's credit file, free of charge, so that no new credit can be opened in your child's name without the use of a PIN number that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your child's credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your child's credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your child's ability to obtain credit. There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your child's credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

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

1. Your child's full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Your child's Social Security number
3. Your child's date of birth
4. If you have moved in the past five years, provide the addresses where your child has 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 your child is a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to place a security freeze on your child's credit report. The credit bureaus must also send written confirmation to you within five business days and provide you with a unique personal identification number ("PIN") or password or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your child's credit report, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (your child's name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your child's credit report or the specific period of time you want the credit report available. The credit reporting agencies have one hour after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to each of the three credit bureaus and include proper identification (your child's name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have one hour after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to remove the security freeze.