



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>>

To <<Name 1>>:

St. Andrew's Episcopal School ("St. Andrew's") writes to inform you of a recent incident that may affect the privacy of some of your information. On Thursday, July 16, 2020, St. Andrew's received notification from one of its 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 St. Andrew's. 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 St. Andrew'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.

What Happened: Blackbaud reported that, in May 2020, it 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 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, St. Andrew's immediately commenced an investigation to determine what, if any, sensitive St. Andrew's data was potentially involved. This investigation included working diligently to gather further information from Blackbaud to understand the scope of the incident. On or about September 29, 2020, St. Andrew's received further information from Blackbaud that more personal information than originally reported was impacted. On or about October 2, 2020, St. Andrew's obtained the details of the additional information impacted from Blackbaud and on December 2, 2020, St. Andrew's confirmed the potentially impacted population.

What Information Was Involved: Our investigation determined that the involved Blackbaud systems contained your name and Social Security number. 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. As part of our ongoing commitment to the security of information in our care, we are working to review 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. We will also be notifying state and federal regulators, as required.

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 and how you can enroll in complimentary credit monitoring.

For More 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 1-800-818-9780, between the hours of 8 am and 8 pm Central Time, Monday through Friday (excluding US holidays). You may also write to St. Andrew's at 1112 West 31st Street Austin, TX 78705.

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

Sincerely,

A handwritten signature in cursive script that reads "Sean Murphy". The signature is written in black ink and is positioned above the printed name and title.

Sean Murphy
Head of School

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll in Credit Monitoring.

Blackbaud has provided 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 notice is sent to you the same day the change or an update takes place with the bureau. In addition, Blackbaud has provided you with proactive fraud assistance to help with any questions you might have. In the event that you are a victim of fraud you will also have access remediation support from a CyberScout Fraud Investigator.

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

<https://www.cyberscouthq.com/epiq263?ac=263HQ1735>

If prompted, please provide the following unique code to gain access to services: **263HQ1735**

Once registered, you can access Monitoring Services by selecting the "Use Now" link to fully authenticate your identity and activate your services. Please remember that in order to receive the monitoring service described above, you must enroll by **March 27, 2021**.

Monitor Your Accounts.

To protect against the possibility of identity theft or other financial loss, we encourage you to remain vigilant, to review your account statements, and to monitor your credit reports for suspicious activity.

Credit Reports.

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.

Security Freeze.

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
PO Box 9554
Allen, TX 75013
1-888-397-3742

TransUnion
P.O. Box 2000
Chester, PA 19016
1-888-909-8872

Equifax
PO Box 105788
Atlanta, GA 30348
1-888-298-0045

www.experian.com/freeze/center.ht www.transunion.com/credi www.equifax.com/personal/credi
ml t-freeze t-report-services

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (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 three (3) business days after receiving your request to remove the security freeze.

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 2002
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
1-888-836-6351

www.equifax.com/personal/credit-report-services

Additional Information.

You can further educate yourself regarding identity theft, and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission.

The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. 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); and TTY: 1-866-653-4261. Instances of known or suspected identity theft should be reported to law enforcement, your state Attorney General, and the FTC. You can also further educate yourself about placing a fraud alert or security freeze on your credit file by contacting the FTC or your state’s 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, www.ncdoj.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.