Appendix

On July 16, 2020, St. Andrew's-Sewanee School ("SAS") was notified by Blackbaud of a ransomware attack on Blackbaud's network that Blackbaud discovered in May of 2020. Blackbaud is a cloud-based software company that provides services to thousands of schools, hospitals, and other non-profits, including SAS. Blackbaud reported that it conducted an investigation, determined that backup files containing information from some of 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 a ransom and obtained confirmation that the stolen files 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, SAS conducted its own investigation to determine what information was involved in the Blackbaud incident. Initially, Blackbaud represented to SAS 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 SAS of its updated findings on September 29, 2020. SAS worked with Blackbaud to identify the individuals whose information may have been involved and determined on October 16, 2020, that the backup files contained certain unencrypted information, including the names and Social Security numbers of five Maine residents. SAS then completed a thorough search for the information needed to notify those involved, which was completed on December 21, 2020.

Beginning today, January 26, 2021, SAS is providing written notice to the Maine residents by mailing letters via United States Postal Service First-Class mail.[1] A sample copy of the notification letter is enclosed. Through Blackbaud, SAS is offering a complimentary, two-year membership of credit monitoring and identity theft prevention services provided by CyberScout. SAS is recommending that the individuals remain vigilant to the possibility of fraud by reviewing their account statements for unauthorized activity. SAS has also notified the three major consumer reporting agencies and established a dedicated phone number where the individuals may obtain more information regarding the incident.

Blackbaud has informed SAS that it identified and fixed the vulnerability associated with this incident, implemented several changes that will better protect data, and is undertaking additional efforts to improve the security of its environment through enhancements to access management, network segmentation, and deployment of additional endpoint and network-based monitoring tools.

[1] This report does not waive St. Andrew's-Sewanee School's objection that Maine lacks personal jurisdiction over it related to any claims that may arise from this incident.

ST. ANDREW'S SEWANEE

<<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>>,

Blackbaud Inc. ("Blackbaud"), the software company that provides St. Andrew's-Sewanee School's ("SAS") data management services, notified us that its systems had been compromised by a data security incident. 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 SAS. On July 16, 2020, Blackbaud first 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 a 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 incident. Initially, Blackbaud told SAS that the fields in the database backups containing personal information were encrypted and not accessible by the unauthorized individual. However, Blackbaud informed SAS of updated findings on September 29, 2020, which indicated that certain information had not been encrypted. SAS worked with Blackbaud to identify the individuals whose information may have been involved and determined on October 16, 2020, that the unencrypted information included certain information pertaining to you. We then completed a thorough search for the information needed to notify those involved, which was completed on December 21, 2020.

What Information Was Involved?

The backup file involved contained your name and Social Security number. Blackbaud informed 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. **For more information on steps you can take in response, including enrolling in the Identity Monitoring and Fraud Resolution services being offered at no cost to you, please see the additional information provided in the following pages.**

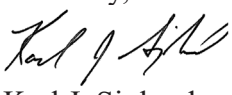
What We Are Doing.

We are notifying you of this incident and sharing the steps that Blackbaud is 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.

SAS regrets that such an incident has occurred and apologizes for any resulting inconvenience. If you have any questions or concerns, please do not hesitate to contact our dedicated helpline at 1-XXX-XXX-XXXX, Monday through Friday, from 9:00 am to 6:30 pm, Eastern Time.

Sincerely,



Karl J. Sjolund
Head of School

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:
https://www.cyberscouthq.com/epiq263?ac=263HQ1733.

If prompted, please provide the following unique code to gain access to services: **263HQ1733**

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:

- *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 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

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts 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 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.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your 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

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Additional information for residents of the following states:

Connecticut: You may contact and obtain information from your state attorney general at: *Connecticut Attorney General's Office*, 165 Capitol Ave, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

North Carolina: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov.

Rhode Island: This incident involves one Rhode Island resident. Under Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov.

West Virginia: You have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.

A Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street NW, Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited.
- You must give your consent for reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a 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.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.