17978

[DATE]

[NAME]
[ADDRESS]
[CITY] [STATE], [ZIP]

SALISBURY
SCHOOL

RE: Notice of Data Breach

Dear _____:

We are writing to advise you of a recent data security incident involving a software company called Blackbaud, Inc. ("Blackbaud"). Salisbury School contracts with Blackbaud to store student, alumni, employee, vendor, and donor information for purposes of donor communications, student record management, and financial management services.

What Happened:

On September 29, 2020, Salisbury School received a notification from Blackbaud informing Salisbury School that a recent ransomware incident at Blackbaud may have resulted in access to certain personal information of our students, alumni, employees, vendors, and donors. We have been informed by Blackbaud that this ransomware incident occurred approximately between February 9, 2020 and May 20, 2020 and that Blackbaud discovered the incident on May 14, 2020.

It is our understanding that this incident has impacted many hundreds of independent schools, colleges and universities, and nonprofit organizations worldwide. The incident did not affect any Salisbury School system or network.

What We Are Doing:

Upon learning of the incident, we reviewed our internal records to identify who may have been affected. We also worked with Blackbaud to obtain additional information about the nature of the event to determine the risk to your personal information.

Types of Information Involved:

Based upon its investigation of the incident, Blackbaud determined that the cybercriminal gained access to certain data, including the unencrypted names, addresses, dates of birth, contact information, Social Security numbers (which may have been used as a vendor tax ID, and bank account numbers of certain Salisbury School students, alumni, donors, employees, and vendors, as a result of the ransomware event. We determined that some of your aforementioned personal information may have been affected by the incident.

What You Can Do:

At this time, we have no reason to believe that Salisbury School information was targeted or that your personal information has, or will be, disseminated or misused in any way. We were also informed that Blackbaud paid a ransom to ensure that any affected personal information was destroyed and not retained. Nevertheless, Salisbury School is taking this matter very seriously and is committed to ensuring your peace of mind.

To that end, through Blackbaud, Salisbury School is offering access to Single Bureau Credit Monitoring services, as well as identity theft protection services, **at no charge**. Services are for twenty-four (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 to remediation support from a CyberScout Fraud Investigator. **In order for you to receive the monitoring service described above, you must enroll within ninety (90) days from the date of this letter**.

To enroll in Credit Monitoring services at no charge, please navigate to:
https://www.cyberscouthq.com/epiq266?ac=266HQ1680
If prompted, please provide the following unique code to gain access to services: **266HQ1680**

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.**

We have also included some general educational information regarding protecting your identity in the enclosed "Reference Guide."

For More Information:

We sincerely regret that this incident occurred and apologize for any inconvenience or concern this incident might cause. If you have any questions, we have set up a dedicated call center to assist you. Please call [insert phone number] between the hours of 8:00 a.m. and 5:00 p.m. EST.

Sincerely,
Chisholm S. Chandler '11 (Hon.) P'17, P'24

Reference Guide

Monitor Account Statements. Remember to look at your account statements regularly to be sure they are correct.

Order Your Free Credit Report. To order your free credit report, visit www.annualcreditreport.com, call toll-free at (877) 322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three credit bureaus provide free annual credit reports only through the website, toll-free number or request form.

When you receive your credit report, review it carefully. Look for accounts you did not open and bills you do not recognize. Look in the "inquiries" section for names of creditors from whom you haven't requested credit. Some companies bill under names other than their store or commercial names. The credit bureau will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in your information (such as home address and Social Security number). If you see anything you do not understand, call the credit bureau at the telephone number on the report. Errors in this information may be a warning sign of possible identity theft. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing.

If you find items you don't understand on your report, call the relevant credit bureau at the number given on the report. Credit bureau staff will review your report with you. If the information can't be explained, then you will need to call the creditors involved. Information that can't be explained also should be reported to your local police or sheriff's office because it may signal criminal activity.

Contact the U.S. Federal Trade Commission. If you detect any unauthorized transactions in your financial account, promptly notify your payment card company or financial institution. If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities, your state Attorney General and the FTC. If you believe your identity has been stolen, the FTC recommends that you take these additional steps:

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. Use the FTC's ID Theft Affidavit (available at www.ftc.gov/idtheft) when you dispute new unauthorized accounts.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft (including information about fraud alerts and security freezes):

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW

Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft

For a summary of your rights under the federal Fair Credit Reporting Act, please visit: https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.

Place a Fraud Alert on Your Credit File. To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free fraud numbers provided below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three credit bureaus. [*The table below contains the contact information relevant to fraud alerts.*]

Equifax	P.O. Box 740241 Atlanta, Georgia 30374-0241	877-478-7625	www.equifax.com
Experian	P.O. Box 9532 Allen, Texas 75013	888-397-3742	www.experian.com
TransUnion	Fraud Victim Assistance Division P.O. Box 2000 Chester, PA 19016	800-680-7289	www.transunion.com

Place a "Security Freeze" on Your Credit File (for Non-Massachusetts Residents). You also may wish to place a "security freeze" (also known as a "credit freeze") on your credit file. A security freeze generally will prevent creditors from accessing your credit file at the three nationwide credit bureaus without your consent. There is no longer a fee for placing, lifting, and/or removing a security freeze. Unlike a fraud alert, you must place a security freeze on your credit file at each credit bureau individually. Since the instructions for establishing a security freeze differ from state to state, please contact the three national credit bureaus to find out more information. [*The table below contains the contact information relevant to security freezes.*]

Equifax	P.O. Box 105788 Atlanta, Georgia 30348	877-478-7625	www.equifax.com
Experian	P.O. Box 9554 Allen, Texas 75013	888-397-3742	www.experian.com
TransUnion	Attn: Security Freeze P.O. Box 160 Woodlyn, PA 19094	888-909-8872	www.transunion.com

The credit bureaus may require proper identification prior to honoring your request. For example, you may be asked to provide:

- Your full name with middle initial and generation (such as Jr., Sr., II, III)
- Your Social Security number
- Your date of birth
- Your complete address including proof of current address, such as current utility or telephone bill
- If you have moved in the past two (2) years, give your previous addresses where you have lived for the past two years
- A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)

Additional Information for Maryland Residents.
You can also obtain information about preventing and avoiding identity theft from the Maryland Attorney General's Office:

Office of the Maryland Attorney General
Identity Theft Unit
200 St. Paul Place, 25th Floor
Baltimore, MD 21202
1-888-743-0023
idtheft@oag.state.md.us
http://www.marylandattorneygeneral.gov

Additional Information for North Carolina Residents.
You can also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-5-NO-SCAM
www.ncdoj.gov

Additional Information for Rhode Island Residents.
Under Rhode Island law, you have the right to file a police report regarding this incident and obtain a copy of it. You can contact the Rhode Island Attorney General to learn more about how to protect yourself from becoming a victim of identity theft:

Office of the Rhode Island Attorney General
Consumer Protection Unit
150 South Main Street
Providence, RI 02903
(401) 274-4400
consumers@riag.ri.gov
http://www.riag.ri.gov

Additional Information for Massachusetts Residents.

Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

Massachusetts law also allows consumers to place a security freeze on their credit reports. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. There is no longer a fee for placing, lifting, and/or removing a security freeze.

To place a security freeze on your credit report, you must send a written request to **each** of the three major consumer reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com) by regular, certified or overnight mail at the addresses below:

- Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348
- Experian Security Freeze P.O. Box 9554 Allen, TX 75013
- Trans Union Security Freeze Fraud Victim Assistance Department P.O. Box 2000 Chester, PA 19022-2000

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.)

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) 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 credit report, you must call or send a written request to the credit reporting agencies 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 as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

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.

Additional Information for District of Columbia Residents.
You can also obtain information about preventing and avoiding identity theft from the Office of the Attorney General for the District of Columbia:
Office of the Attorney General
400 6th Street NW
Washington, D.C. 20001
(202) 727-3400
oag@dc.gov
https://oag.dc.gov/

Additional Information for New York Residents.
You can also obtain information about preventing and avoiding identity theft from the New York Attorney
General's Office:
Office of the Attorney General
The Capitol
Albany, NY 12224-0341
1-800-771-7755
https://ag.ny.gov/our-office