EXHIBIT 1

The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Randolph School does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

Nature of the Data Event

On October 14, 2020, Randolph School received notification from one of its former third-party vendors, Blackbaud, of a cyber incident. Blackbaud is a cloud computing provider that provides financial services tools to organizations, including Randolph School. Blackbaud reported that, in May 2020, it experienced an attempted ransomware incident that resulted access to 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 reported that the threat actor was able to exfiltrate data from Blackbaud's network at some point before Blackbaud locked the unauthorized actor out of the environment on May 20, 2020. While Blackbaud discovered this activity in May 2020, it was not until October 14, 2020 that Blackbaud notified Randolph School that the unknown actor may have accessed or acquired certain Blackbaud customer data related to the Randolph School.

Upon receiving notice of the cyber incident, Randolph School immediately commenced an investigation to better understand the nature and scope of the incident and any impact on Randolph School data. This investigation included working diligently to gather further information from Blackbaud to understand the scope of the incident and to assess the risk to any Randolph School data stored on impacted systems. Blackbaud reported that this information had been transferred into an unencrypted state without Randolph School's knowledge, and this information may have been accessible to the unauthorized actor. On October 22, 2020, Blackbaud provided Randolph School the records containing the information from the potentially impacted systems it had identified. While Blackbaud did not confirm if this information had been subject to unauthorized access or acquisition, it could not rule out the possibility of such activity.

On October 22, 2020, Blackbaud provided this updated information, at which time, Randolph School confirmed that it included name, address, and Social Security number for one (1) Maine resident. Thereafter, Randolph School worked to confirm the appropriate contact information and provide notice to potentially impacted individuals as quickly as possible.

Notice to Maine Resident

On or about November 20, 2020, Randolph School began providing written notice of this incident to affected individuals, which includes one (1) Maine resident. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, Randolph School moved quickly to investigate and respond to the incident, assess the security of Randolph School systems, and notify potentially affected individuals. Randolph School is also working to implement additional safeguards and training to its employees. Randolph School is providing access to credit monitoring services for 24 months through CyberScout to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Randolph School is providing impacted individuals with guidance on how to better protect against identity theft and fraud. Randolph School is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, 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.

EXHIBIT A

RANDOLPH

[Date]

[First Name] [MI] [Last Name] [Suffix]
[Address Line 2]
[Address Line 2]
[City, State] [Zip Code]

Dear [First Name] [MI] [Last Name] [Suffix]:

Randolph School writes to make you aware of a recent incident at a former third-party vendor, Blackbaud, Inc. ("Blackbaud"), that may affect the privacy of some of your information. *While we have no evidence of any actual or attempted misuse of any information as a result of this incident*, this notice provides information about the Blackbaud incident, our response and efforts to obtain additional information from Blackbaud, and resources available to you to help protect your information from possible misuse, should you feel it necessary to do so.

What Happened? On October 14, 2020, Randolph School received notification from one of our former third-party vendors, Blackbaud, of a cyber incident. Blackbaud is a cloud computing provider that provides financial services tools to organizations, including Randolph School. Randolph terminated the relationship with Blackbaud in April 2019 over a year prior to this incident. Blackbaud reported that, in May 2020, it experienced an attempted ransomware incident that resulted in access to 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 reported that the threat actor was able to exfiltrate data from Blackbaud's network at some point before Blackbaud locked the unauthorized actor out of the environment on May 20, 2020. While Blackbaud discovered this activity in May 2020, it was not until October 14, 2020 that Blackbaud notified Randolph School that the unknown actor may have accessed or acquired certain Blackbaud customer data related to Randolph School.

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 Randolph School data. This investigation included working diligently to gather further information from Blackbaud to understand the scope of the incident and to assess the risk to any Randolph School data stored on impacted systems. Blackbaud reported that this information had been transferred into an unencrypted state without Randolph School's knowledge, and this information may have been accessible to the unauthorized actor. On or about October 22, 2020, Blackbaud provided Randolph School the records containing the information from the potentially impacted systems it had identified. While Blackbaud did not confirm if this information had been subject to unauthorized access or acquisition, it could not rule out the possibility of such activity.

What Information Was Involved? Our investigation determined that the potentially impacted information included your name and [variable data element]. Please note that, to date, we have not received confirmation from Blackbaud that your specific information was accessed or acquired by an unknown actor.

What Are We 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 procedures regarding our third-party vendors. Randolph School is continuing to work with Blackbaud to address relevant questions and the next steps that Blackbaud is taking to remediate its data privacy event. Please note that Blackbaud confirmed it will be removing this historical unencrypted information from its network. We will also be notifying state regulators, as required.

1005 Drake Avenue SE, Huntsville, Alabama 35802
Phone: 256-799-6100 • Fax: 256-881-1784
www.randolphschool.net

Although Randolph School is unaware of any actual or attempted misuse of your information as a result of this incident, Blackbaud is offering you access to credit monitoring services for 24 months at no cost to you as an added precaution. Please note that you must complete the enrollment process yourself, as we are not permitted to enroll you in these services on your behalf.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your credit reports for suspicious activity and to detect errors. We also 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 a description of services and instructions on how to enroll in these services.

For More Information. We understand that you may have questions about the Blackbaud incident that are not addressed in this letter. If so, please contact Randolph School at bbinfo@randolphschool.net.

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

Sincerely,

RANDOLPH SCHOOL

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll in Credit Monitoring

As an added precaution, Blackbaud is 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, Blackbaud is 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 within 90 days from the date of this letter.

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.)

Enrollment Instruction

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=263HQ1647

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

263HQ1647

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 within 90 days from the date of this letter.

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 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.

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
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion
P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872
www.transunion.com/credit-freeze

Equifax
P.O. Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
www.equifax.com/personal/credit-report-services

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.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

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 9554
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
1-888-766-0008
www.equifax.com/personal/credit-report-services

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; 1-877-ID-THEFT (1-877-438-4338); and 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.