



Dear [REDACTED],

Rumsey Hall School ("Rumsey") values and respects the privacy of your information, which is why we are writing to advise you of a recent data security incident involving a company called Blackbaud, Inc. ("Blackbaud"). Rumsey contracts with Blackbaud to manage our donor, alumni, and vendor databases within Blackbaud's self-hosted environment.

What Happened? Blackbaud recently notified us, as well as hundreds of other organizations that use its products, that it was impacted by a ransomware event. According to Blackbaud, in May 2020, an unauthorized third party deployed ransomware within Blackbaud's environment and some of its data was exfiltrated out of its systems.

What Information Was Involved? On or around October 13, 2020, Blackbaud informed us that the unauthorized individual who gained access to Blackbaud's network could have accessed files that contained your name and Tax Identification Number ("TIN"). In addition, if you use your Social Security number as your TIN, as it relates to your professional engagement with Rumsey, your Social Security number may have also been impacted by the incident. Since that time, we have been reviewing the information provided by Blackbaud, working to locate addresses, and working to contact individuals regarding the incident. **At this point, we have received no indication that your information has been misused for fraud or identity theft.** Nonetheless, we are providing you with this notice because your personal information may have been involved in the incident.

What We Are Doing: Upon learning of the incident, we reviewed our internal records to determine if your personal information was potentially affected by the incident. We also worked with Blackbaud to obtain additional information about the nature of the event. We are committed to taking steps to help prevent this from happening again; including reviewing our relationship with Blackbaud, and the technical controls they have in place for securing our data.

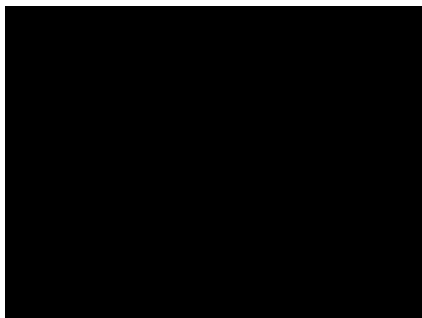
What You Can Do: Although we are not aware of any instances of fraud or identity theft, we are offering, through Blackbaud, a complimentary two-year membership of Single Bureau Credit Monitoring through CyberScout, LLC ("CyberScout"). This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. Single Bureau Credit Monitoring through CyberScout is completely free to you, and enrolling in this program will not hurt your credit score. **For more information on identity theft prevention and Single Bureau Credit Monitoring through CyberScout, including instructions on how to activate your complimentary two-year membership, please see the additional information provided in this letter.**

Other Important Information: We recommend that you remain vigilant to protect against potential fraud by, among other things, reviewing your account statements and credit reports closely. If you detect any suspicious activity, you should promptly notify the financial institution or company with which the account is maintained. While we have no evidence that anyone's personal information has been misused, you can find more information on steps to protect

yourself against identity theft or fraud in the enclosed *Additional Important Information* sheet.

For More Information: We value the trust you place in us and take our responsibility to safeguard your personal information seriously. We apologize for any inconvenience or concern this incident might cause. For further assistance, please call [REDACTED], from 9:00 AM to 6:30 PM Eastern Time, Monday through Friday.

Sincerely,



Credit Monitoring Information

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 within 90 days from the date of this letter.

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 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.)

Additional Important Information

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Credit Reports: You may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies by visiting www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at <https://www.annualcreditreport.com/manualRequestForm.action>.

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is as follows:

Equifax 1-866-349-5191 www.equifax.com P.O. Box 740241 Atlanta, GA 30374	Experian 1-888-397-3742 www.experian.com P.O. Box 9554 Allen, TX 75013	TransUnion 1-800-888-4213 www.transunion.com P.O. Box 1000 Chester, PA 19016
---	--	--

Fraud Alerts: You may want to consider placing a fraud alert on your credit report. A fraud alert is free and will stay on your credit report for one (1) year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at www.annualcreditreport.com.

Credit and Security Freezes: You may have the right to place a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax Security Freeze 1-888-298-0045 www.equifax.com P.O. Box 105788 Atlanta, GA 30348	Experian Security Freeze 1-888-397-3742 www.experian.com P.O. Box 9554 Allen, TX 75013	TransUnion Security Freeze 1-888-909-8872 www.transunion.com P.O. Box 160 Woodlyn, PA 19094
---	--	---

Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by requesting information in writing from the Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. NW, Washington, DC 20580.

This notice was not delayed by law enforcement.

Maryland Residents: Maryland residents can contact the Office of the Attorney General to obtain information about steps you can take to avoid identity theft from the Maryland Attorney General's office at: Office of the Attorney General, 220 St. Paul Place, Baltimore, MD 21202, (888) 743-0023.

New York State Residents: New York residents can obtain information about preventing identity theft from the New York Attorney General's Office at: Office of the Attorney General for the State of New York, Bureau of Consumer Frauds & Protection, The Capitol, Albany, New York 12224-0341; <https://ag.ny.gov/consumer-frauds/identity-theft>; (800) 771-7755.