150 N. Riverside Plaza, Suite 3000, Chicago, IL 60606 • (312) 819-1900

January 29, 2021

Bruce A. Radke
(312) 463-6211
(312) 819-1910
bradke@polsinelli.com

VIA E-MAIL (ATTORNEYGENERAL@DOJ.NH.GOV)
AND FEDERAL EXPRESS

The Honorable Gordon MacDonald
Attorney General of the State of New Hampshire
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notification of a Data Security Incident

Dear Attorney General MacDonald:

We represent Colgate Rochester Crozer Divinity School ("CRCDS") in connection with a recent incident that may have impacted the personal information of one (1) New Hampshire resident, and we provide this notice on behalf of CRCDS pursuant to N.H. REV. STAT. ANN. § 359-C:20. This notice will be supplemented, if necessary, with any new significant facts discovered subsequent to its submission. While CRCDS is notifying you of this incident, CRCDS does not waive any rights or defenses relating to the incident or this notice, or the applicability of New Hampshire law on personal jurisdiction.

NATURE OF THE SECURITY BREACH OR UNAUTHORIZED USE OR ACCESS

On July 16, 2020, CRCDS's cloud service provider, Blackbaud Inc. ("Blackbaud") notified CRCDS that it was impacted by a ransomware event. According to Blackbaud, ransomware was deployed within its environment in May 2020, and certain data was exfiltrated out of its systems between April 18, 2020 and May 7, 2020. At the time, Blackbaud first reported the incident to CRCDS in July, Blackbaud said that most of the exfiltrated data (including any data that might be considered sensitive) was encrypted and therefore not viewable by the unauthorized person even after it was exfiltrated. However, on September 29, 2020, Blackbaud alerted CRCDS that in fact certain Social Security numbers that it had initially thought were encrypted when exfiltrated were actually unencrypted and therefore viewable by the unauthorized party. Upon learning this new information from Blackbaud, CRCDS immediately began reviewing its internal records to identify who may have been affected.

CRCDS is not aware of any fraud or identity theft to any individual as a result of this incident but is notifying the potentially impacted residents.

NUMBER OF NEW HAMPSHIRE RESIDENTS AFFECTED

The incident may have impacted one (1) New Hampshire resident. CRCDS mailed notification letters to these individuals on today, January 29, 2021. Enclosed is a sample of the notice that is being sent to the impacted residents via first-class United States mail.

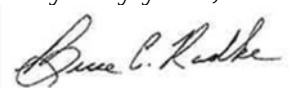
STEPS TAKEN RELATING TO THE INCIDENT

Upon learning of the incident, CRCDS worked to get additional information from Blackbaud about the incident and the potentially impacted information so that it could notify potentially impacted individuals. CRCDS is also providing complimentary identity theft protection services to the impacted individual through Blackbaud's CyberScout services. Finally, CRCDS is reviewing its relationship with Blackbaud and the technical controls in place for securing CRCDS's data in the Blackbaud systems.

CONTACT INFORMATION

Please contact me if you have any questions or if I can provide you with any further information concerning this matter.

Very truly yours,



Bruce A. Radke

Enclosure

Colgate Rochester Crozer Divinity School
Mail Handling Services
777 E Park Dr
Harrisburg, PA 17111

Colgate Rochester Crozer
DIVINITY SCHOOL

[redacted]

January 28, 2021

Dear [redacted]:

Colgate Rochester Crozer Divinity School ("Colgate" or "we") values and respects the privacy of your information, which is why we are writing to advise you of a recent incident that may have involved some of your personal information. We have no reason to believe that your personal information has been misused for the purpose of committing fraud or identity theft. Nonetheless, we are writing to advise you of a recent security event involving a company called Blackbaud, Inc. ("Blackbaud") that may have involved information about you.

Over the years, Colgate, like many other educational institutions, has contracted with Blackbaud to provide a variety of products that help us manage certain student, applicant, employee, and vendor data. On July 16, 2020, Blackbaud notified us (as well as hundreds of other organizations that use its products) that it was impacted by a ransomware event. According to Blackbaud, ransomware was deployed within its environment in May 2020, and certain data was exfiltrated out of its systems between April 18, 2020 and May 7, 2020. At the time, Colgate did not realize what data was affected in Blackbaud's ransomware incident.

On September 29, 2020, Blackbaud alerted us that it had additional findings. In this follow up notice, and to our frustration, Blackbaud explained that data that was exfiltrated was actually unencrypted and therefore viewable by the unauthorized party. This unencrypted data, Blackbaud reported, included certain individuals' Social Security numbers. Upon learning this new information from Blackbaud, we immediately began reviewing our internal records to identify who may have been affected. Our review concluded that your name and Social Security were within the data set that the unauthorized person could have accessed.

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 from 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.

We value the trust you place in us and apologize for any inconvenience or concern this incident might cause. Please know that we are taking steps to help prevent this from happening again, including reviewing our relationship with Blackbaud and the technical controls that it has in place for securing our data. If you need further assistance, please call 1-844-305-8392 from 8 a.m. to 5 p.m. Eastern, Monday through Friday.

Sincerely,

Paula Blue

Paula Blue
Vice President for Institutional Effectiveness
Colgate Rochester Crozer Divinity School

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	Experian	TransUnion
1-866-349-5191	1-888-397-3742	1-800-888-4213
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	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	Experian Security Freeze	TransUnion Security Freeze
1-888-298-0045	1-888-397-3742	1-888-909-8872
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094

Iowa Residents: Iowa residents can contact the Office of the Attorney general to obtain information about steps to take to avoid identity theft from the Iowa Attorney General's office at: Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines IA 50319, 515-281-5164.

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.

North Carolina Residents: North Carolina residents can obtain information about preventing identity theft from the North Carolina Attorney General's Office at: North Carolina Attorney General's Office, 9001 Mail Service Center, Raleigh, NC 27699-9001, (877) 566-7226.

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.

Rhode Island Residents: We believe that this incident affected two (2) Rhode Island residents. Rhode Island residents can contact the Office of the Attorney general at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, (401) 274-4400.

Vermont Residents: If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).

Credit Monitoring Enrollment

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.)