BAKER DONELSON
BEARMAN, CALDWELL & BERKOWITZ, PC

CHASE NORTH TOWER
450 LAUREL STREET
21ST FLOOR
BATON ROUGE, LOUISIANA
70801

PHONE: 225.381.7000
FAX: 225.343.3612

www.bakerdonelson.com

LAYNA S. COOK RUSH, SHAREHOLDER
Direct Dial: 225.381.7043
Direct Fax: 225.382.0243
E-Mail Address: lrush@bakerdonelson.com

August 17, 2020

Via Email

Attorney General Bob Ferguson
Washington State Office of the Attorney General
1125 Washington Street SE
PO Box 40100
Olympia, WA 98054-0100
SecurityBreach@atg.wa.gov

Re: Third Party Vendor Data Incident

Dear Attorney General Ferguson:

Please be advised that the undersigned and the law firm of Baker, Donelson, Berman, Caldwell & Berkowitz, PC represent Colby College with regard to a third party vendor data incident that may have impacted personal information for some Washington residents.[1] Colby College received notification from Blackbaud, Inc. ("Blackbaud") on July 16, 2020 that Blackbaud discovered and stopped a ransomware attack of Blackbaud's self-hosted platform in May, 2020. Blackbaud is the global market leader in third-party donor applications used by many charities, health and educational organizations in the U.S. and abroad.

According to Blackbaud, prior to being locked out, the cybercriminals removed a copy of sensitive data from its self-hosted environment which contained information related to individuals affiliated with multiple charitable institutions. Blackbaud reports that it paid the cybercriminals' demand and received confirmation that the copy of the data removed has been destroyed. According to Blackbaud, this incident occurred at some point between February 7, 2020 and May 20, 2020 and was discovered in May of 2020.

Upon notice of this incident, Colby College promptly sent an email communication on July 26, 2020 to its constituents alerting them to this incident. Working with counsel, Colby College

[1] By providing this notice, Colby College does not waive any rights or defenses regarding the applicability of your State's law, the applicability of your State's data event notification statute, or personal jurisdiction.

reviewed its files and records to determine what personal information related to its constituents may have been impacted.

Based on an extensive review of its files and records, Colby College determined that the name, address and date of birth for six hundred and six (606) Washington residents may have been impacted by this incident. Contemporaneous with this notification, Colby College is sending written notice to the six hundred and six (606) Washington residents.

Blackbaud has stated that based on the nature of the incident, its research and third-party investigation, including investigation by law enforcement, it has no reason to believe that any data went beyond the cybercriminals, was or will be misused, or will be disseminated or otherwise made available publicly. Blackbaud reports it has hired a third-party team of experts to monitor the web as an extra precautionary measure. Additionally, we have been informed by Blackbaud that it has implemented numerous security changes. Specifically, Blackbaud stated that it quickly identified the vulnerability associated with this incident and took swift action to fix it. Blackbaud also stated that it has confirmed through testing by multiple third parties that its fix withstands all known attack tactics. Finally, Blackbaud has asserted that it is further hardening its environment through enhancements to access management, network segmentation, deployment of additional endpoint and network-based platforms.

Colby College continues to review all relevant business practices regarding the security of Blackbaud data and will continue to monitor the situation and provide relevant updates to its constituents as appropriate.

For more information regarding this incident, please see the sample notification letter included herewith. Additionally, an account of the incident may be found at blackbaud.com/securityincident. Should you have any questions regarding the foregoing or need more information, please contact the undersigned.

Sincerely,

BAKER, DONELSON, BEARMAN,
CALDWELL & BERKOWITZ, PC

By: Layna C. Rush

Layna C. Rush

LCR:krc
Enclosure (Breach Notification Letter)

<<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

August 17, 2020

RE: Notice of Third-Party Data Incident

Dear <<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>,

On July 26, 2020, many of you received an e-mail from Colby College alerting you to a data breach suffered by Blackbaud, Inc., a leading provider of cloud software and data management used by Colby and many other colleges, universities and non-profit organizations. Much of this letter repeats the information provided in that notice, but for those who may not have received the initial e-mail, we thought the information was worth repeating. Additionally, through our work with counsel engaged by the College that concentrate on data breaches, we have been able to determine more clearly the personal data pertinent to you which may have been exposed as a result of the Blackbaud incident. If you have questions, I invite you to contact me directly.

What happened?

On July 16, 2020, we were notified that Blackbaud, an outside vendor of Colby College, discovered and stopped a ransomware attack of Blackbaud's self-hosted platform in May 2020. Blackbaud is the global market leader in third party donor applications used by many charities, health, and educational organizations in the U.S. and abroad.

According to Blackbaud, prior to being locked out, the cybercriminal removed a copy of a subset of data from its self-hosted environment which contained information related to individuals affiliated with multiple charitable institutions. Blackbaud reports that it paid the cybercriminal's demand and received confirmation that the copy of the data removed has been destroyed. According to Blackbaud, this incident occurred at some point between February 7, 2020 and May 20, 2020 and was discovered in May of 2020.

What information was involved?

The backup file that was removed may have contained names and contact information, along with some demographic information, related to a number of Colby College's donors. Based on review of our records, your first and last name, address and date of birth may have been involved in the incident.

Blackbaud has stated that based on the nature of the incident, its research, and third-party investigation, including investigation by law enforcement, it has no reason to believe that any data went beyond the cybercriminal, was or will be misused, or will be disseminated or otherwise made available publicly. Blackbaud reports it has hired a third-party team of experts to monitor the web as an extra precautionary measure.

What are we doing?

As we noted in our July 26 e-mail, the College takes the issue of data security very seriously. Since our previous notice, we have been reviewing all relevant business practices regarding the security of Blackbaud data with the assistance of breach counsel. We have been informed by Blackbaud that it has implemented numerous security changes. Specifically, Blackbaud stated that it quickly identified the vulnerability associated with this incident and took swift action to fix it. Blackbaud also stated that it has confirmed through testing by multiple third parties that its fix withstands all known attack tactics. Finally, Blackbaud has asserted that it is further hardening its environment through enhancements to access management, network segmentation, deployment of additional endpoint and network-based platforms. That said, we will continue to monitor the situation and provide relevant updates.

What can you do?

We do not think there is anything more you need to do at this time. It is always best practice to routinely monitor your personal accounts for unusual activity and to contact the appropriate financial institution or service provider if you have concerns. For your convenience, we have included information on actions you may take if you are concerned about unusual activity with your personal accounts.

For more information about this incident, you can consult the Blackbaud website at blackbaud.com/securityincident. If you have additional questions about this incident, please contact the College at advancement@colby.edu or 207-859-4336. Thank you for your partnership and continued support.

Jane B. Phillips '01,

Vice President for College Advancement

Below are additional actions you may take, if you feel it is necessary.

➢ **FREEZE YOUR CREDIT FILE.** 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. 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. Note that a security freeze generally does not apply to existing account relationships and when a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of account review, collection, fraud control or similar activities. There is no charge to place or lift a security freeze.
To place a security freeze on your credit report, contact each of the three major consumer reporting agencies using the contact information listed below:

3 MAJOR CREDIT BUREAUS / CONSUMER REPORTING AGENCIES

Equifax	**Experian**	**TransUnion**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
1-800-525-6285	1-888-397-3742	1-800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

To request a security freeze, you will need to provide the following:

- Your full name (including middle initial as well as Jr., Sr., II, III, etc.), Social Security number, and date of birth;
- If you have moved in the past five (5) years, the addresses where you have lived over the prior five years;
- Proof of current address, such as a current utility bill or telephone bill;
- A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.); and
- 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.

If you request a security freeze via toll-free telephone or other secure electronic means, the credit reporting agencies have one (1) business day after receiving the request to place the freeze. In the case of a request made by mail, the bureaus 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 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 a 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 the request to remove the freeze.

➢ **PLACE FRAUD ALERTS ON YOUR CREDIT FILE.** As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on your credit 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 an alert lasting 7 years. Contact the credit reporting agencies listed above to activate an alert.

➢ **REMAIN VIGILANT: REVIEW YOUR ACCOUNT STATEMENTS, & REPORT FRAUD.** Carefully review your credit reports, debit/credit card, insurance policy, bank account and other account statements. Activate alerts on your bank accounts to notify you of suspicious activity. Report suspicious or fraudulent charges to your insurance statements, credit report, credit card or bank accounts to your insurance company, bank/credit card vendor and law enforcement. (For Oregon & Iowa residents: Report any suspected identity theft to law enforcement, Federal Trade Commission, and your State Attorney General.)

➢ **ORDER YOUR FREE ANNUAL CREDIT REPORTS.** Visit www.annualcreditreport.com or call 877-322-8228 to obtain one free copy of your credit report annually. Periodically review a copy of your credit report for discrepancies and identify any accounts you did not open or inquiries you did not authorize. (For Colorado, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain additional copies of your credit report, free of charge. You must contact each of the three credit reporting agencies directly to obtain such additional reports.)

➢ **POLICE REPORT:** You have a right to a police report about this incident (if any exists). If you're an identity theft victim, you have the right to file a police report and obtain a copy of it.

➢ **OBTAIN INFORMATION ABOUT PREVENTING IDENTITY THEFT FROM FTC / STATE ATTORNEY GENERAL.** Go to http://www.experian.com/credit-advice/topic-fraud-and-identity-theft.html. The Federal Trade Commission also provides information at www.ftc.gov/idtheft. The FTC can be reached by phone: 1 - 877-438-4338; TTY: 1-866-653-4261 or by writing: 600 Pennsylvania Ave., NW, Washington, D.C. 20580. Your State Attorney General also may provide information. For North Carolina residents: You may contact North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

➢ **FILE YOUR TAXES QUICKLY AND SUBMIT IRS FORM 14039.** If you believe you are at risk for taxpayer refund fraud, the IRS suggests you file your income taxes quickly. Additionally, if you are an actual or potential victim of identity theft, the IRS suggests you give them notice by submitting IRS Form 14039 (Identity Theft Affidavit). This form will allow the IRS to flag your taxpayer account to alert them of any suspicious activity. Form 14039 may be found at https://www.irs.gov/pub/irs-pdf/f14039.pdf.

➢ **FAIR CREDIT REPORTING ACT:** You also have rights under the federal Fair Credit Reporting Act (FCRA), which promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. The FTC has published a list of the primary rights created by the FCRA (https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf), and that article refers individuals seeking more information to visit www.ftc.gov/credit. The FTC's list includes the following FCRA rights: (1) To receive a copy of your credit report, which must contain all the information in your file at the time of your request; (2) To receive a free copy of your credit report, at your request, once every 12 months from each of the nationwide credit reporting companies – Equifax, Experian, and TransUnion; (3) To receive a free credit report if a company takes adverse action against you (e.g. denying your application for credit, insurance, or employment), and you ask for your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the credit reporting company. You are also entitled to one free report a year if you are unemployed and plan to look for a job within 60 days; if you are on welfare; or if your report is inaccurate because of fraud, including identity theft; (4) To ask for a credit score; (5) To dispute incomplete or inaccurate information; (6) To obtain corrections to your report or delete inaccurate, incomplete, or unverifiable information; (7) Consumer reporting agencies may not report outdated negative information; (8) To restrict access to your file and to require consent from you for reports to be provided to employer; (9) To limit "prescreened" offers of credit and insurance you receive based on information in your credit report; and (10) To seek damages from violators. Please note that identity theft victims and active duty military personnel may have additional rights under the FCRA.

➢ **PROTECT YOURSELF FROM PHISHING SCAMS.** Learn to recognize phishing emails. Do not open emails from unknown senders and be sure not to click on strange links or attachments. Never enter your username and password without verifying the legitimacy of the request by contacting the sender by telephone or other methods. Replying to the email is not a safe way to confirm. Visit https://www.consumer.ftc.gov/articles/0003-phishing for more information on these types of scams.