BakerHostetler

Baker&Hostetler LLP
Key Tower
127 Public Square, Suite 2000
Cleveland, OH 44114-1214

T 216.621.0200
F 216.696.0740
www.bakerlaw.com

David E. Kitchen
direct dial: 216.861.7060
dkitchen@bakerlaw.com

November 4, 2020

VIA OVERNIGHT MAIL

Attorney General Gordon MacDonald
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Incident Notification

Dear Attorney General MacDonald:

We are writing on behalf of our client, Stuart Country Day School of the Sacred Heart ("Stuart School"), to notify you of a security incident involving New Hampshire residents. Stuart School is an independent all-girls Catholic country day school that serves students from pre-kindergarten through twelfth grade.

On July 16, 2020, Stuart School was notified by Blackbaud of a ransomware attack on Blackbaud's network that the company discovered in May of 2020. Blackbaud is a cloud-based software company that provides services to thousands of schools, hospitals, and other non-profits. Blackbaud reported that it conducted an investigation, determined that backup files containing information from some of its clients had been taken from its network, and an attempt was made to encrypt files to convince Blackbaud to pay a ransom. Blackbaud paid a ransom and obtained confirmation that the stolen files had been destroyed. Blackbaud also reported that it has been working with law enforcement.

Upon learning of the incident from Blackbaud, Stuart School conducted its own investigation of the Blackbaud services used by Stuart School and the information provided by Blackbaud to determine what information was involved in the incident. On September 9, 2020, Stuart determined that the backup files contained certain information pertaining to two New Hampshire residents including the residents' name and financial account number.

Beginning today, November 4, 2020, Stuart School is providing written notice to the New Hampshire residents by mailing letters via United States Postal Service First-Class mail.[1] A sample copy of the notification letter is enclosed. Stuart School is recommending that the individuals remain vigilant to the possibility of fraud by reviewing their account statements for unauthorized activity. Stuart School has also established a dedicated phone number where the individuals may obtain more information regarding the incident.

Blackbaud has informed Stuart School that they identified and fixed the vulnerability associated with this incident, implemented several changes that will better protect data and are undertaking additional efforts to improve the security of its environment through enhancements to access management, network segmentation, and deployment of additional endpoint and network-based platforms.

Please do not hesitate to contact me if you have any questions regarding this incident.

Sincerely,

David E. Kitchen
Partner

Enclosure

[1] This report does not waive Stuart School's objection that New Hampshire lacks personal jurisdiction over it related to any claims that may arise from this incident.

STUART
COUNTRY DAY SCHOOL OF THE SACRED HEART

C/O IDX
10300 SW Greenburg Rd. Suite 570
Portland, OR 97223

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

To Enroll, Please Call:
1-800-939-4170
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code:
<<XXXXXXXX>>

November 4, 2020

Dear <<First Name>> <<Last Name>>,

We are writing to notify you that Stuart Country Day School of the Sacred Heart and many other institutions were notified by Blackbaud, Inc. that it experienced a security incident. This notice explains the incident and measures taken in response.

What Happened?
Blackbaud is a cloud-based software company that provides services to thousands of schools, hospitals, and other non-profits, including Stuart Country Day School of the Sacred Heart. On July 16, 2020, Blackbaud notified us that it had discovered an attempted encryption attack on Blackbaud's network in May 2020. Blackbaud reported that it conducted an investigation and determined that backup files containing information from its clients had been taken from its network. Blackbaud paid a ransom and obtained confirmation that the files that had been removed by the unauthorized actor had been destroyed. Blackbaud also reported that it has been working with law enforcement. Upon learning of the incident from Blackbaud, we conducted our own investigation to determine what information was involved in the incident. Based upon this investigation, on September 9, 2020, we determined that the backup files contained certain information pertaining to you.

What Information Was Involved?
The backup file involved contained your [Variable Text]. Blackbaud has assured us that the backup file has been destroyed by the unauthorized individual and there is no reason to believe any data was or will be misused, disseminated, or otherwise be made available publicly.

What We Are Doing:
We are notifying you of this incident and sharing the steps that we and Blackbaud are taking in response. Blackbaud has informed us that it identified and fixed the vulnerability associated with this incident, implemented several changes that will better protect your data from any subsequent incidents, and is undertaking additional efforts to harden its environment through enhancements to access management, network segmentation, and deployment of additional endpoint and network-based monitoring tools. We have also undertaken to enhance our internal measures to better ensure that, if sensitive information is stored in our records, it is maintained through means that cannot be accessed without authorization.

What You Can Do:
While we have no evidence that your personal information has been misused, we wanted to let you know this happened and assure you we take it very seriously. In addition, we are offering you complimentary identity theft protection services through IDX. IDX protection services include: 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised. You can enroll in the complimentary IDX protection services being offered to you by calling 1-800-939-4170 or going to https://app.idx.us/account-creation/protect and using the Enrollment Code provided above. IDX experts are available Monday through Friday from 6 am - 6 pm Pacific Time. Please note the deadline to enroll

is February 4, 2021. IDX representatives can answer questions or concerns you may have regarding protection of your personal information.

For More Information:
We regret that this occurred and apologize for any inconvenience. Please note, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Should you have any further questions or concerns regarding this incident, please call our dedicated helpline at 1-800-939-4170, Monday through Friday from 6 am - 6 pm Pacific Time.

Sincerely,

Rose S. Neubert
Chief Financial & Operating Officer

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.
For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Additional information for residents of the following states:

New York: You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection,* One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220.
http://www.dos.ny.gov/consumerprotection; and *New York State Office of the Attorney General,* The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov.

North Carolina: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 /1-877-566-7226, www.ncdoj.gov.