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 25, 2020

VIA FIRST CLASS MAIL

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

Re: Incident Notification

Dear Mr. MacDonald:

We are writing on behalf of our client, St. Lawrence University, to notify you of a security incident involving New Hampshire residents. St. Lawrence University is a private liberal arts college located in Canton, NY.

On July 16, 2020, St. Lawrence University was notified by Blackbaud of a ransomware attack on Blackbaud's network that the company discovered in May of 2020. Blackbaud is a 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, St. Lawrence University conducted its own investigation of the Blackbaud services used by St. Lawrence University and the information provided by Blackbaud to determine what information was involved in the incident. On October 12, 2020, St. Lawrence University determined that the backup files contained certain information pertaining to 6 New Hampshire residents, including the residents' name and financial account number.

Beginning today, November 25, 2020, St. Lawrence University 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. St. Lawrence University is recommending that the individuals remain vigilant to the possibility of fraud by reviewing their account statements for unauthorized activity. St. Lawrence University has also established a dedicated phone number where the individuals may obtain more information regarding the incident.

Blackbaud has informed St. Lawrence University 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 field-, file- and database-level encryption; and data retention procedures. St. Lawrence University has put additional systems in place to further maintain the confidentiality of constituent information and has also performed a thorough review of all of its security and data retention procedures.

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 St. Lawrence University's objection that New Hampshire lacks personal jurisdiction over it related to any claims that may arise from this incident.

St. Lawrence University
Mail Handling Services
777 E Park Dr
Harrisburg, PA 17111

ST. LAWRENCE UNIVERSITY

[redacted]

November 25, 2020

Dear [redacted]:

St. Lawrence University is writing to notify you of a data security incident that occurred at one of our vendors, Blackbaud, Inc. ("Blackbaud"). This notice explains the incident and measures taken in response.

What Happened?
Blackbaud is a software company that provides services to thousands of schools, hospitals, and other non-profits, including St. Lawrence University. On July 16, 2020, Blackbaud notified us and many other institutions that it had discovered an attempted ransomware attack on Blackbaud's network in May 2020. Blackbaud reported that it conducted an investigation, determined that backup files containing information from 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 files removed had been destroyed. The time period of unauthorized access was between February 7 to May 20, 2020. Blackbaud reported that it has been working with law enforcement, including the FBI. Since learning of the incident from Blackbaud on July 16, 2020, we diligently conducted our own investigation of the Blackbaud services we use and the information provided by Blackbaud to determine what information was involved in the incident. We engaged legal counsel to assist in that investigation and worked with Blackbaud to identify the individuals whose information may have been involved. On October 12, 2020, we determined that the backup files contained certain unencrypted information pertaining to you. Therefore, we are providing you with this notification of the incident.

What Information Was Involved?
The backup file involved contained your name, routing number, and financial account number ending in [redacted] and [redacted]. Blackbaud 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 or will be disseminated or otherwise made available publicly.

What You Can Do:
Even though 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. For more information, including additional steps you can take in response, please see the additional information provided in the following pages.

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 they identified and fixed the vulnerability associated with this incident, implemented several changes that will better protect your data from any subsequent incidents, and are undertaking additional efforts to harden their environment through enhancements to field-, file- and database-level encryption; and data retention procedures.

As a University, we have put additional systems in place to further maintain the confidentiality of constituent information. We have also performed a thorough review of all of our security and data retention procedures.

For More Information:
We deeply regret that this happened and apologize for any inconvenience this may have caused. Should you have any further questions or concerns, please do not hesitate to contact us at 1-888-781-3999, Monday through Friday from 8am to 5pm Eastern Time.

Sincerely,

Rich Basler, CFRE
Executive Director of Advancement Operations

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.

If your health insurance or medical information was involved, it is also advisable to review the billing statements you receive from your health insurer or healthcare provider. If you see charges for services you did not receive, please contact the insurer or provider immediately.

Additional information for residents of the following states:

Connecticut: You may contact and obtain information from your state attorney general at: *Connecticut Attorney General's Office,* 165 Capitol Ave, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag

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