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

February 25, 2021

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, Families in Transition, to notify you of a security incident that occurred at one of its vendors, Blackbaud, Inc. ("Blackbaud").

Families in Transition is a homeless services organization in New Hampshire, with locations in Manchester, Concord, Dover and Wolfeboro. Blackbaud is a cloud-based software company that provides services to thousands of schools, hospitals, and non-profits, including Families in Transition.

Families in Transition was notified by Blackbaud on July 16, 2020 that it had discovered a ransomware attack on Blackbaud's network in May 2020. Families in Transition stopped using Blackbaud products in 2019, before this incident took place; however, Blackbaud had maintained a backup file of Families in Transition data. Blackbaud reported that it conducted an investigation, determined that there had been unauthorized access to its systems between February 7, 2020 and May 20, 2020, 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. On September 29, 2020, Blackbaud provided Families in Transition with additional information about the scope of the incident.

Following receipt of the notifications about the incident from Blackbaud, Families in Transition launched its own investigation to identify the individuals whose information may have

been involved in the Blackbaud incident. Because it no longer used Blackbaud's products, a forensic review firm was engaged to search and review the backup file. Families in Transition subsequently determined that the Blackbaud backup files contained certain information pertaining to some of its constituents, including their names and one or more of the following: Social Security numbers, driver's license numbers, and credit card numbers.

Beginning today, February 25, 2021, Families in Transition is mailing notification letters to 29 New Hampshire residents via United States Postal Service First-Class mail. A copy of the notification letter is enclosed. Families in Transition is offering the New Hampshire residents with Social Security numbers or driver's license numbers involved complimentary, one-year memberships to credit monitoring and identity theft prevention services through Experian. Families in Transition has established a phone number where the individual may obtain more information regarding the incident.

Families in Transition no longer maintains its data on Blackbaud databases. Regarding the backup file, Blackbaud has informed Families in Transition 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

[Letterhead]

[NAME 1]
ADDRESS OF [NAME 1]
CITY, STATE, ZIP

[DATE]

Dear [NAME 1]:

Families in Transition is writing to notify you that we and many other institutions were notified by Blackbaud 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. On July 16, 2020, Blackbaud notified us that it had discovered a ransomware attack on Blackbaud's network in May 2020. Families in Transition stopped using Blackbaud products in 2019, before this incident took place; however, Blackbaud had maintained a backup file of Families in Transition data. Blackbaud reported that it conducted an investigation, determined there had been unauthorized access to its systems between February 7, 2020 to May 20, 2020, 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 that had been removed had been destroyed. Blackbaud reported that it has been working with law enforcement.

Upon learning of the incident from Blackbaud, we conducted our own investigation of the Blackbaud services we used and the information provided by Blackbaud to determine what information was involved in the incident. Because we no longer use Blackbaud's products, we engaged a forensic review firm to search and review the backup file. On December 16, 2020, we determined that the backup files contained certain information pertaining to you.

What Information Was Involved
The backup file involved contained your [Variable Data]. 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 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. As a precaution, we are offering you a complimentary membership of Experian's® IdentityWorks℠. This product provides you with identity detection and resolution of identity theft. IdentityWorks is completely free to you and enrolling in this program will not hurt your credit score. For more information on IdentityWorks, including instructions on how to activate your complimentary one-year membership, as well as some 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 access management, network segmentation, and deployment of additional endpoint and network-based platforms. Again, Families in Transition no longer maintains its data on Blackbaud databases.

For More Information
We regret that this occurred and apologize for any inconvenience. Should you have any further questions or concerns regarding this matter, please do not hesitate to contact me at phawkes@fitnh.org or at 603-641-9441 ext. 324.

Sincerely,

[SIGNATURE IMAGE]
Pamela Hawkes
Vice President Resource Development

Activate IdentityWorks Now in Three Easy Steps

1. ENROLL by: **5/31/2021** (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: www.experianidworks.com/3bcredit
3. PROVIDE the **Activation Code:** [Code]

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **(877) 890-9332.** Be prepared to provide engagement number **B009904** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Activate your membership today at www.experianidworks.com/3bcredit
or call (877) 890-9332 to register with the activation code above.

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at **(877) 890-9332.**

* Offline members will be eligible to call for additional reports quarterly after enrolling.
** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

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.