WILSON ELSER
WILSON ELSER MOSKOWITZ EDELMAN & DICKER LLP

June 16, 2021

Anjali C. Das
312.821.6164 (direct)
Anjali.Das@wilsonelser.com

Via Online Submission

Attorney General Aaron Frey
Office of the Attorney General
6 State House Station
Augusta, ME 04333

Re: Cybersecurity Incident Involving Blackbaud, Inc., Third Party Vendor for Little Hill Foundation for the Rehabilitation of Alcoholics, Inc. d/b/a Alina Lodge

Dear Attorney General Frey:

We represent Little Hill Foundation for the Rehabilitation of Alcoholics, Inc. d/b/a Alina Lodge ("Alina Lodge"), a HIPAA covered, non-profit organization that offers alcohol and drug addiction treatment and rehabilitation services located in Blairstown, New Jersey. As discussed below, this cybersecurity incident involves one of Alina Lodge's third party vendors, Blackbaud, Inc. ("Blackbaud"). Alina Lodge takes the security and privacy of its alumni and guarantors information seriously, and although Alina Lodge will provide notice pursuant to HIPAA, Alina Lodge wanted to inform you as soon as possible of this incident given it received confirmation of 7 potentially impacted Maine residents.

1. **Nature of the incident.**

Blackbaud is a cloud computing provider that is used by Alina Lodge, and many other institutions, to organize and store information related to members of its community.

On October 15, 2020, Alina Lodge received the first notification letter dated October 6, 2020 from Blackbaud regarding a cybersecurity incident which resulted in the exposure of personal information maintained by the institutions on the Blackbaud platform. A copy of Blackbaud's notice of the incident is attached here as **Exhibit A**. Additionally, Blackbaud published its summary of the incident on its website at www.blackbaud.com/securityincident. Upon learning about the incident, Alina Lodge immediately started an investigation to determine the scope and extent of information potentially involved in the incident.

Alina Lodge's investigation included numerous communications with Blackbaud between October 2020 and April 19, 2021 to seek clarity about what specific data concerning Alina Lodge and its clients may have been compromised as a result of the cyber attack on Blackbaud. Based on communications from Blackbaud, it was Alina Lodge's understanding that all of our client information stored by Blackbaud was encrypted and not accessible by any unauthorized party.

However, on April 19, 2021, Blackbaud confirmed to Alina Lodge, for the first time, that Alina Lodge's client information was not in fact encrypted – with the exception of social security numbers.

After an internal investigation, Alina Lodge discovered the three Blackbaud platforms used by Alina Lodge, *Raiser's Edge NXT*, *Financial Edge NXT*, and *Research Point*¸ stored information of its 2,565 alumni and guarantors. Of these 2,565 alumni and guarantors, 7 were Maine residents whose information stored on the impacted Blackbaud platforms may have included: the name, address, phone number, date of birth, admission/discharge date, and other limited treatment information. As confirmed by Blackbaud, all social security numbers were stored in an encrypted format for security purposes. Thus, according to Blackbaud, no social security numbers were exposed to any unauthorized parties as a result of this incident.

At this time, based on the information that Alina Lodge received from Blackbaud, Alina Lodge has no reason to believe that any personal information of its alumni or guarantors have been misused as a result of this incident.

2. Number of Maine residents affected.

7 Maine residents were potentially affected by the incident. An incident notification letter addressed to the Maine residents will be mailed pursuant to HIPAA. A sample copy of the notification letter being mailed to potentially affected residents of Maine is included with this letter at **Exhibit B**.

3. Steps taken in Response to the Incident.

Alina Lodge takes the security and privacy of all alumni and guarantors information very seriously, and has taken steps to protect the privacy and security of potentially impacted individuals' information. Specifically, Alina Lodge informed our law firm, Wilson Elser Moskowitz Edelman & Dicker LLP, and began identifying the individuals contained within the Blackbaud platforms used by Alina Lodge in preparation for notice.

As outlined in the sample notification to the impacted individual, Alina Lodge provided the impacted individuals with complimentary services to help protect their identity. Specifically, Alina Lodge has arranged for the impacted individuals to enroll in credit monitoring and cyber monitoring services (including identity theft protection) provided by TransUnion Interactive, a subsidiary of TransUnion, at no cost to them for 12 months.

Moreover, Blackbaud has indicated that it has taken (or plans to take) the following steps to strengthen its cybersecurity post-attack:

- Hardening Blackbaud's environment through enhancements to access management, network segmentation, and deployment of additional endpoint and network-based platforms;
- Steps to improve to the granularity of reporting at both the host and network level to ensure intrusion detection capabilities;

- Accelerating efforts to add multi-factor authentication to all of Blackbaud's self-hosted solutions;
- Ensuring all users reset their passwords regularly;
- Requiring stronger user passwords for certain customers;
- Increasing efforts to migrate customers to Cloud environments (including Microsoft Azure and Amazon Web Services.

4. **Contact information.**

Alina Lodge remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Anjali.Das@WilsonElser.com or 312-821-6164.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

Anjali C. Das

Enclosure

Exhibit A

blackbaud®

October 6, 2020

Little Hill Foundation, Inc.
ATTN: Head of IT Department
PO Box G
Blairstown, NJ 07825-0966

Re: Notification of Security Incident

Dear Customer,

We are writing to ensure you are aware of a particular security incident that recently occurred. On July 16, 2020, your organization received an email from Blackbaud regarding this incident. We are sending you this letter by postal mail as required by our contract with your organization and/or because we have been unsuccessful in our attempts to contact someone from your organization. We are truly sorry this incident occurred and are committed to working directly with your organization to provide the support you need.

What Happened

In May of 2020, we discovered and stopped a ransomware attack. In a ransomware attack, cybercriminals attempt to disrupt the business by locking companies out of their own data and servers. After discovering the attack, our Cyber Security team—together with independent forensics experts and law enforcement—successfully prevented the cybercriminal from blocking our system access and fully encrypting files; and ultimately expelled them from our system.

Prior to our locking the cybercriminal out, the cybercriminal removed a copy of a subset of data from our self-hosted (private cloud) environment. Because protecting our customers' data was our top priority, we paid the cybercriminal's demand with confirmation that the copy they removed had been destroyed.

Based on the nature of the incident, our research, and third party (including law enforcement) investigation, we have 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. In accordance with regulatory requirements and in an abundance of caution, we are notifying all organizations whose data was part of this incident and are providing resources and tools to help them assess this incident. You can read more at www.blackbaud.com/securityincident.

What This Means for Your Organization Specifically

Our public cloud environment (Microsoft Azure and Amazon Web Services) and most of our self-hosted (private cloud) datacenters, products and customers were not part of this incident, but we have confirmed the following specific to your organization:

- A copy of your Blackbaud Financial Edge NXT®, Blackbaud Raiser's Edge NXT® and ResearchPoint™ backups were part of this incident.

We did discover that the cybercriminal may have had access to some fields intended for sensitive information. Specifics for your organisation, what we are doing about it, and next steps are included below.

Situation: (Situation ID: FE Bank Account # in Treasury) The Bank Account field in the Treasury module of Financial Edge/Financial Edge NXT was unencrypted. This field stores your organization's bank account number.

> **What Blackbaud is doing to address this:** We intend to encrypt the Bank Account field of the Treasury module by the end of October.
>
> **The action your organization needs to take:** We have created instructions on how to query the Bank Account field of the Treasury module. Once we give your organization access to your solutions, copy this link into your browser for those instructions: https://kb.blackbaud.com/articles/Knowledge/194365. Please contact Customer Support if you need help with these instructions.

And again, based on the nature of the incident, our research, and third party (including law enforcement) investigation, we have 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. We have hired a third-party team of experts to monitor the dark web as an extra precautionary measure.

In the email we sent to your organization on July 16, 2020, we provided a link to a secured page that has various resources for your organization. You can access that page by visiting https://www.blackbaud.com/incidentresources. On that page, we have provided a toolkit with a step-by-step guide to help you as you digest this information. It also contains answers to key questions, links to educational webinars, information about our future plans, and other resources. Your toolkit provides a written guide to notification laws and access to a webinar that helps you assess potential notification requirements in your jurisdictions. We advise you to also consult with your organization's legal counsel to understand any notification requirements. If you determine that you do need to notify your constituents, we have included templates in your toolkit to make it easier.

In the meantime, we encourage you to review the resources we provided in the link above. If you have additional questions, please contact us at the corresponding email address below:

- **For US-based customers, email** CustomerSuccess@blackbaud.com
- **For all other customers, email** customersuccess@blackbaud.ca

We understand this situation is frustrating. This was a very sophisticated attack, and while we were able to defend against it for the most part, we realize this is still requiring that you invest time to review the situation, and that you may need to invest time to take follow-up actions. Again, we apologize for this and will continue to do our very best to supply help and support as we and our customers jointly navigate any necessary response to the cybercriminal's actions.

Sincerely,
Blackbaud

Exhibit B

ALINA LODGE

Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Re: Notice of Security Incident

Dear <<Name 1>>:

Little Hill Foundation for the Rehabilitation of Alcoholics, Inc. – "Alina Lodge" – is dedicated to the lifelong recovery of the individuals seeking care with us. Out of an abundance of caution, we are writing to inform you of a data security incident involving one of our vendors, Blackbaud, Inc. ("Blackbaud"), that may have resulted in the exposure of some of your personal data. The data does not include medical information or notes from any therapy sessions. Please know we take the security of your information very seriously. Alina Lodge sincerely apologizes for any inconvenience this incident may cause you. This letter contains information about the incident and steps you can take to further protect your information.

Who is Blackbaud:

Blackbaud is a cloud computing provider that is used by Alina Lodge, and other institutions, to organize and store information related to clients and members of our community.

What happened:

On October 15, 2020, Alina Lodge received a notification letter from Blackbaud regarding a cybersecurity incident resulting in the compromise of certain data stored by Blackbaud on its computer systems. Upon learning about the incident, Alina Lodge immediately started an investigation to determine the nature and scope of information potentially involved in the Blackbaud incident. Blackbaud confirmed on multiple occasions during our investigation that our data was encrypted, and therefore not viewable. On April 19, 2021, Blackbaud confirmed to Alina Lodge, for the first time, that some of Alina Lodge's client data might have been exposed. No Social Security numbers or credit card data were exposed to any unauthorized parties as a result of this incident.

What information was involved:

Personal data including your name, address, phone number, date of birth, admission/discharge date, and other limited treatment information, including diagnoses or recovery status, may have been viewed by an unauthorized individual. At this time, based on the information that Alina Lodge has received from Blackbaud, Alina Lodge has no reason to believe that any personal information of members of the Alina Lodge community has been misused as a result of this incident. As confirmed by Blackbaud, no Social Security numbers or credit card data were exposed to any unauthorized parties as a result of this incident.

The information that may have been viewed by an unauthorized individual was contained in records affiliated with our philanthropic department, with data that was stored specifically for donor purposes. Like other nonprofits, we store this data to allow us to cultivate potential gifts to support our mission. While some personal data was contained in these records, no data from our medical/clinical records was stored in Blackbaud at any time.

What we are doing and what you can do:

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*my*TrueIdentity) for one year provided by TransUnion Interactive, a subsidiary of TransUnion,® one of the three nationwide credit reporting companies.

How to Enroll: You can sign up online or via U.S. mail delivery.

- To enroll in this service, go to the *my*TrueIdentity website at **www.MyTrueIdentity.com** and, in the space referenced as "Enter Activation Code," enter the 12-letter Activation Code **<< Activation Code>>** and follow the three steps to receive your credit monitoring service online within minutes.

- If you do not have access to the Internet and wish to enroll in a similar offline, paper-based credit monitoring service, via U.S. mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the six-digit telephone passcode **<<Engagement Number>>** and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and **<<Enrollment Deadline>>**. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH COMPLIMENTARY CREDIT MONITORING SERVICE:

- Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score.

- The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more.

- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

Alina Lodge also refers you to the *Additional Important Information* section of this letter, which provides you with further information to obtain your credit report, place fraud alerts and freeze your credit.

For more information:

The protection of your information is our top priority, and Alina Lodge sincerely regrets any inconvenience that this matter may cause you. If you have any questions, please call the following toll-free number: 855-866-8964. Representatives are available to assist you from 9:00 am to 9:00 pm Eastern time, Monday through Friday.

Sincerely,

William Robbins, LCSW
Executive Director

Additional Important Information

For residents of *Hawaii*, *Michigan*, *Missouri*, *Virginia*, *Vermont*, and *North Carolina*: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of *Illinois*, *Iowa*, *Maryland*, *Missouri*, *North Carolina*, *Oregon*, and *West Virginia*:
It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of *Iowa*:
State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *Oregon*:
State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of *Maryland*, *Rhode Island*, *Illinois*, *New York and North Carolina:*
You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023
www.oag.state.md.us

Rhode Island Office of the Attorney General
Consumer Protection
150 South Main Street
Providence RI 02903
1-401-274-4400
www.riag.ri.gov

North Carolina Office of the Attorney General
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-566-7226
www.ncdoj.com

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

New York Office of the Attorney General
Bureau of Consumer Frauds & Protection
The Capitol
Albany, NY 12224-0341
1-800-771-7755
https://ag.ny.gov/consumer-frauds/identity-theft

For residents of *Washington*: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of all states:
Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf); TransUnion (https://www.transunion.com/fraud-alerts); or Experian (https://www.experian.com/fraud/center.html). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
www.freeze.equifax.com
800-525-6285

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
www.experian.com/freeze
888-397-3742

TransUnion (FVAD)
P.O. Box 2000
Chester, PA 19022
freeze.transunion.com
800-680-7289

More information can also be obtained by contacting the Federal Trade Commission listed above.