

Appendix

Beech Acres Parenting Center (“Beech Acres”) is a charitable organization that inspires and equips today's parents, families, and communities to raise capable, caring, contributing children in Cincinnati, Ohio. Blackbaud, Inc. (“Blackbaud”) is a cloud-based software company that provides services to Beech Acres as well as thousands of other schools, hospitals, and non-profit organizations.

Beech Acres was notified by Blackbaud on July 16, 2020 of a ransomware attack on Blackbaud’s network that the company discovered in May of 2020. Blackbaud reported that the attack took place between February 7, 2020 to May 20, 2020. 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. On September 29, 2020, Blackbaud provided Beech Acres with additional information about the scope of the incident.

Following receipt of the notifications about the incident from Blackbaud, Beech Acres conducted its own investigation of the Blackbaud services used by Beech Acres and the information provided by Blackbaud to determine what information was involved in the incident. On November 5, 2020, Beech Acres determined that the backup files potentially contained personal information. Beech Acres subsequently identified information pertaining to two Maine residents, including the residents’ name and financial account number.

Beginning today, January 15, 2021, Beech Acres is providing written notice to the Maine residents by mailing letters via United States Postal Service First-Class mail.¹ A sample copy of the notification letter is enclosed. Beech Acres is recommending that the individuals remain vigilant to the possibility of fraud by reviewing their account statements for unauthorized activity. Beech Acres has also established a dedicated phone number where the individuals may obtain more information regarding the incident.

Blackbaud has informed Beech Acres 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.

¹ This report does not waive Beech Acres’ objection that Maine lacks personal jurisdiction over it related to any claims that may arise from this incident.



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Dear <<first_name>>,

As a valued member of Beech Acres Parenting Center's donor family, I am writing today to inform you of a database security incident that we learned of last summer. We and many other institutions were notified by Blackbaud, our constituent database vendor, of this incident. This notice explains the incident and measures taken in response.

Please know that Beech Acres Parenting Center takes the utmost care with the confidential information that is a part of our business, including the donor information that is part of our Blackbaud database system. Once we were notified of this data breach, we took the necessary time to research and evaluate the situation with the assistance of our information security and management consulting firm in order to assess what information of our donors may have been involved. Please note this as the reason that many married couples will each receive their own letter.

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. 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 use and the information provided by Blackbaud to determine what information was involved in the incident. On November 5, 2020, we determined that the backup files contained certain information pertaining to you. Since that time, we have been working with our vendors to compile address information and produce notification letters.

What Information Was Involved

The backup file involved contained your name and financial account number ending in <<b2b_text_1(exposed information)>>. 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 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. Beech Acres Parenting Center is also reviewing our vendor relationships and will continue to handle confidential information with the utmost care pursuant to our procedures and policies to protect the financial information that you entrust to us when you make a donation.

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.

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 call 1-833-971-3301 Monday through Friday 9:00am to 6:30pm Eastern Time. You can also contact our Vice President of Development, Patty Rosely, at prosely@beechacres.org or 513.233.4748.

Thank you for placing your trust in Beech Acres to deliver the help that children and families need to thrive. I hope with the steps outlined above you continue to trust that Beech Acres will continue to take the utmost care with your confidential information.

Sincerely,

A handwritten signature in black ink, appearing to read "Jim", is positioned above the typed name and title.

James R. Mason
President & CEO

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:

Rhode Island: [This incident involves 1 Rhode Island resident.](#) Under Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov

A Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited.
- You must give your consent for reports to be provided to employers.
- You may limit “prescreened” offers of credit and insurance you get based on information in your credit report.
- 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.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.