EXHIBIT 1

We write on behalf of Berkshire to notify your office of an incident that may affect the security of some personal information related to three (3) Maine residents. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Berkshire does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

Nature of the Data Event

On July 16, 2020, Berkshire received a communication from one of its third-party vendors, Blackbaud, Inc. ("Blackbaud"), notifying Berkshire of a cyber incident. Blackbaud is a cloud computing provider that offers customer relationship management and financial services tools to organizations, including Berkshire. Upon receiving notice of the cyber incident, Berkshire immediately commenced an investigation to better understand the nature and scope of the incident and any impact on Berkshire data. This investigation included working diligently to gather information from Blackbaud to understand the scope of the incident. Berkshire received further information on subsequent dates, including July 27, 2020 and September 1, 2020, that allowed it to confirm the information potentially affected by the incident, and that the information may have contained protected personal information.

In its initial communication, Blackbaud reported that, in May 2020, it experienced a ransomware incident that resulted in encryption of certain Blackbaud systems. Blackbaud reported the incident to law enforcement and worked with forensic investigators to determine what occurred. Following its investigation, Blackbaud notified its customers that an unknown actor may have accessed or acquired certain Blackbaud customer data. Blackbaud reported that the data was exfiltrated by the threat actor at some point before Blackbaud locked the threat actor out of the environment on May 20, 2020. Based on Berkshire's investigation, it was determined that the information that could have been subject to unauthorized acquisition includes name and Social Security number.

Notice to Maine Residents

On or about September 22, 2020, Berkshire provided written notice of this incident to affected individuals, which include three (3) Maine residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, Berkshire moved quickly to investigate and respond to the incident and to notify potentially affected individuals. This included extensive coordination with Blackbaud to confirm what information could have been potentially affected that may have contained personal information. Berkshire is working to review existing policies and procedures regarding third-party vendors and is working with Blackbaud to evaluate additional measures and safeguards to protect against this type of incident in the future. Berkshire is providing individuals whose personal information was potentially affected by this incident with access to one year of credit monitoring services through ID Experts at no cost to those individuals.

Additionally, Berkshire is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Berkshire is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. Berkshire will also be notifying other state regulators as required.

EXHIBIT A

BERKSHIRE
FARM CENTER & SERVICES FOR YOUTH

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

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

<<Full Name>>
<<Address 1>> <<Address 2>>
<<City>>, <<State>> <<Zip Code>>

September 22, 2020

Dear <<Full Name>>:

Berkshire Farm Center & Services for Youth, Inc. ("Berkshire") writes to inform you of a recent incident involving Blackbaud, Inc. ("Blackbaud") a third-party vendor that Berkshire uses for database assistance in donor relations and fundraising operations, as well as financial operations. On July 16, 2020, Berkshire received notification from Blackbaud of a cyber incident that Blackbaud uncovered in May 2020. The confidentiality, privacy, and security of information in our care are among our highest priorities, and we take this incident very seriously.

Upon receiving notice of the cyber incident, Berkshire immediately began an investigation to better understand the nature and scope of the incident and any impact on Berkshire's data. This notice provides information about the Blackbaud incident, our response, and resources available to you to help protect your information from possible misuse, should you feel it necessary to do so.

Blackbaud reported that, in May 2020, two months before notifying Berkshire, it discovered a ransomware incident that resulted in encryption of certain Blackbaud systems. Blackbaud reported the incident to law enforcement and worked with forensic investigators to determine the nature and scope of the incident. Blackbaud notified its customers, including Berkshire, that a cybercriminal may have accessed or acquired certain Blackbaud customer data. Blackbaud reported that the data was potentially exported by the threat actor before Blackbaud locked the cybercriminal out of its environment on May 20, 2020. According to Blackbaud the data was destroyed, and they do not believe that any data was or will be misused, disseminated or otherwise be made publicly available. Blackbaud further stated that this belief has been corroborated by outside experts and law enforcement.

Berkshire has worked diligently to gather further information from Blackbaud to understand the incident. Our own investigation determined that the involved Blackbaud systems may have contained your <<Information Impacted>>. We have not received any information from Blackbaud that your information was specifically accessed or acquired by the cybercriminal.

Your private information and its security are of the utmost importance to Berkshire. We are reviewing our existing policies and procedures regarding our third-party vendors, and are working with Blackbaud to evaluate additional measures and safeguards to protect against this type of incident in the future. As an added precaution, we are offering you with access to <<CM Length>> of credit monitoring through ID Experts MyIDCare at no cost to you. Additional details on services and instructions for enrolling are included in the enclosed *Steps You Can Take to Help Protect Your Information.*

While we have no reason to believe there are any specific actions you need to take in this situation, we encourage you to review the enclosed *Steps You Can Take to Help Protect Your Information*. There you will find general information on what you can do to help protect your personal information. We encourage you to review account statements and explanation of benefits forms and report any suspicious activity to the institution that issued that statement immediately.

We understand that you may have questions about the Blackbaud incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 1-800-939-4170 Monday through Friday between the hours of 9:00 am to 9:00 pm Eastern Time. You may also write to Berkshire at 13640 State Route 22, Canaan, NY 12029.

We sincerely regret any inconvenience or concern this incident has caused.

Sincerely,

Bailey Naples

Bailey Naples
Chief Compliance Officer

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll in Credit Monitoring

As an added precaution, we are offering identity theft protection services through ID Experts®, the data breach and recovery services expert, to provide you with MyIDCare™. MyIDCare services include: <<CM Length>> of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised.

1. **Website and Enrollment.** Go to https://app.myidcare.com/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. The deadline to enroll in free MyIDCare services is December 22, 2020.

2. Activate the credit monitoring provided as part of your MyIDCare membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, MyIDCare will be able to assist you.

3. Telephone. Contact MyIDCare at 1-800-939-4170 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

Monitor Your Accounts.

To protect against the possibility of identity theft or other financial loss, we encourage you to remain vigilant, to review your account statements, and to monitor your credit reports and explanation of benefits forms for suspicious activity.

Credit Reports.

Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

Security Freeze.

You have the 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. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	**TransUnion**	**Equifax**
PO Box 9554	P.O. Box 2000	PO Box 105788
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-888-909-8872	1-888-298-0045
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a

consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 2002	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-836-6351
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

Additional Information.

You can further educate yourself regarding identity theft, and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission.

The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue, NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. Instances of known or suspected identity theft should be reported to law enforcement, your Attorney General, and the FTC. You can also further educate yourself about placing a fraud alert or security freeze on your credit file by contacting the FTC or your state's Attorney General. This notice was not delayed by a law enforcement investigation.

For Maryland residents, the Attorney General can be contacted by mail at 200 St. Paul Place, Baltimore, MD, 21202; toll-free at 1-888-743-0023; by phone at (410) 576-6300; consumer hotline (410) 528-8662; and online at www.marylandattorneygeneral.gov. ***For New Mexico residents***, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the 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 credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580. ***For New York residents,*** the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/. ***For North Carolina residents:*** The North Carolina Attorney General can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; toll-free at 1-877-566-7226; by phone at 1-919-716-6400, and online at www.ncdoj.gov.