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

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

<<First Name>> <<Middle>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

November 11, 2020

Dear <<First Name>> <<Last Name>>,

The Orchard School Foundation (the "Orchard School") takes the privacy and security of your information seriously. We are writing to inform you of a security incident experienced by one of our third-party service providers that may have involved some of your information. We want you to understand what we are doing to address this issue and what steps you can take to protect yourself.

What Happened

Blackbaud, Inc. ("Blackbaud"), a third-party service provider that the Orchard School uses for donor relations and fundraising operations, informed us that it experienced a security incident earlier this year. Blackbaud is one of the world's largest providers of education administration, fundraising and financial management software for the non-profit sector.

Blackbaud first notified us in July 2020, that Blackbaud discovered cybercriminals had gained access to Blackbaud's servers and removed data associated with hundreds of Blackbaud's customers, including some Orchard School data. More information about the incident may be found on Blackbaud's website at https://www.blackbaud.com/securityincident. As a client of Blackbaud, we are not privy to all details of the intrusion or the results of Blackbaud's investigation. Our understanding of this incident, the information impacted, and Blackbaud's efforts to contain it, is based entirely on information we have received from Blackbaud over the course of numerous communications.

We understand from Blackbaud that the incident began in early 2020, and is believed to have continued through May 2020, after Blackbaud detected and expelled a cybercriminal from its systems. The cybercriminal accessed and copied a subset of data stored on Blackbaud's systems and demanded a ransom payment in exchange for destroying that information. This data included certain information that the Orchard School maintains with Blackbaud. Blackbaud informed us that it paid a ransom in exchange for confirmation from the cybercriminal that any data that was accessed and copied has been destroyed. Additionally, Blackbaud reports that it is working with US Federal law enforcement and actively monitoring via third party experts, and has found no trace of the data being available. We have no reason to believe at this point that your information was used by, or will be disseminated by, the cybercriminal.

When Blackbaud first informed us of the incident in July 2020, Blackbaud indicated that personal information was not impacted. Nevertheless, we immediately began our own investigation to assess what Orchard School data may have been impacted and worked diligently to gather relevant facts from Blackbaud. We also engaged our own forensics investigator to further analyze the incident. In September 2020, Blackbaud provided additional information indicating that personal information may have been impacted.

What Information Was Involved

Our investigation revealed that some of your personal information may have been accessed by the cybercriminal, including your <<Variable Data 2: Data Elements>>.

Our investigation did not reveal any unauthorized access to any credit card data or bank account information as part of this incident.

What We Are Doing

This security incident was limited to Blackbaud's systems and networks. The Orchard School's own systems and networks were not compromised in this incident. In addition to informing you, we are taking proactive steps with Blackbaud to understand how this occurred and what can be done to prevent a future occurrence. Further, Blackbaud has informed us that they have implemented changes to prevent this specific issue from happening again. You can review more details on Blackbaud's security, risk, compliance and privacy programs at https://www.blackbaud.com/security.

Although we are unaware of any identity theft or fraud stemming from this incident, out of an abundance of caution, we are offering identity theft protection services through IDX, experts in data breach and recovery services. IDX identity protection services include: <<Variable Data 1: Credit Monitoring Duration>> of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do

We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling 1-800-939-4170 or going to https://app.idx.us/account-creation/protect and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is February 11, 2021.

We also encourage you to remain vigilant in monitoring your account statements and financial transactions for incidents of fraud and identity theft, and to promptly report such incidents. Further, please routinely review bills, notices, and statements that you receive from financial institutions.

For More Information

Although there is no evidence that your information was accessed as a result of this incident, if you want to learn more about the steps you can take to protect against identity theft or fraud, please review the enclosed "Reference Guide" materials.

We appreciate your valued support and we regret any inconvenience this may cause you. If you have any questions or need assistance, please go to https://app.idx.us/account-creation/protect or call 1-800-939-4170, toll free Monday through Friday from 9 am - 9 pm Eastern Time. The toll-free number has been created specifically to answer your questions about the incident services.

Sincerely,

Orchard School Foundation

Recommended Steps to help Protect your Information

1. **Website and Enrollment.** Go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection 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, IDX will be able to assist you.

3. Telephone. Contact IDX 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.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. 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. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601**,** www.ag.ky.gov, Telephone: 1-502-696-5300.

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

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 a violator. 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. You can 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.

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/.

North Carolina Residents: Office of the Attorney General of North Carolina**,** 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.