



Return Mail Processing Center
P.O. 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>>

Dear <<Name 1>>:

Re: Notice of Data Breach

University School of Nashville was notified on July 16, 2020 by Blackbaud, a third-party software and data storage service provider, of a data security event that occurred between February and May 2020. Blackbaud provides donor recordkeeping and relationship management services to University School of Nashville, as well as other independent schools, colleges and universities, health care organizations, and foundations within the nonprofit sector.

What Happened? According to Blackbaud, in May they discovered and stopped a ransomware attack. After discovering the attack, Blackbaud's Cyber Security team, together with independent forensic specialists and law enforcement, successfully prevented the cybercriminals from blocking system access and fully expelled them from their systems. Prior to being locked out, the cybercriminals removed a copy of a backup file that may have contained some of your personal information. Additionally, Blackbaud informed us that it paid a ransom in exchange for confirmation that the compromised information has been destroyed. Blackbaud reported that it has taken steps to fortify its systems against any further data security incidents. On or about September 29, 2020, University School of Nashville received further information from Blackbaud that allowed it to determine the information potentially affected may have contained personal information.

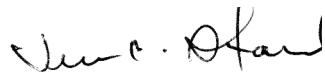
What Information Was Involved. The following personal information related to you was potentially impacted by the incident: your name, address, bank account and routing number, Social Security number and/or tax identification number, which may be your Social Security number. University School of Nashville has no indications that your personal information was misused, disseminated, or otherwise made available publicly. However, out of an abundance of caution, we wanted to advise you of this incident.

What We Are Doing. The confidentiality, privacy, and security of information in our care are among our highest priorities, and we take this incident very seriously. As part of our ongoing commitment to the security of information in our care, we are working to review 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. While we are unaware of any misuse of your information as a result of this incident, we are offering you access to 24 months of credit monitoring and identity restoration services through CyberScout.

What You Can Do. You can find out more about how to protect against potential identity theft and fraud in the enclosed *Steps You Can Take to Protect Your Information*. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements and to monitor your credit reports for suspicious activity. You may also enroll in the complimentary credit monitoring services described above. Enrollment instructions are attached to this letter.

For More Information. We apologize for this incident and regret any inconvenience this may cause you. If you have additional questions, please call our dedicated assistance line at 888-905-0521, Monday through Friday (excluding U.S. holidays), during the hours of 9:00 a.m. to 9:00 p.m., Eastern Time. You may also write to University School of Nashville at 2000 Edgehill Ave, Nashville, TN 37212.

Sincerely,

A handwritten signature in black ink, appearing to read "Teresa Standard". The signature is fluid and cursive, with a large initial "T" and a long, sweeping underline.

Teresa Standard
Chief Financial Officer

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Enrollment Instructions

Single-Bureau Credit Monitoring + Proactive Fraud Assistance + ID Theft and Fraud Resolution + Credit Freeze DBC P20 B109	<p>We are providing you with access to Single Bureau Credit Monitoring services at no charge. Services are 24 months from the date of enrollment. When changes occur to your Experian credit file, notification is sent to you the same day that the change or update takes place with the bureau. In addition, we are providing you with proactive fraud assistance to help with any questions you might have. In the event you become a victim of fraud you will also have access remediation support from a CyberScout Fraud Investigator. In order for you to receive the monitoring service described above, you must enroll within 90 days from the date of this letter.</p> <p><u>How do I enroll for the free services?</u></p> <p>To enroll in Credit Monitoring* services at no charge, please log on to https://www.myidmanager.com and follow the instructions provided. When prompted please provide the following unique code to receive services: 263HQ1897. In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter.</p>
---	--

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. 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.

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

P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion

P.O. Box 2000
Chester, PA 19016
1-888-909-8872
www.transunion.com/credit-freeze

Equifax

P.O. Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial, as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five years, the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, military identification, etc.);
7. If you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

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 one-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

P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion

P.O. Box 2000
Chester, PA 19016
1-800-680-7289
[www.transunion.com/
fraud-victim-resource/place-fraud-alert](http://www.transunion.com/fraud-victim-resource/place-fraud-alert)

Equifax

P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008
[www.equifax.com/personal/
credit-report-services](http://www.equifax.com/personal/credit-report-services)

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

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. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For Maryland residents: The Attorney General may be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662; and www.oag.state.md.us.

For North Carolina residents: The Attorney General may be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

For Rhode Island residents: The Attorney General may be contacted at: 150 South Main Street, Providence, Rhode Island 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 3 Rhode Island residents impacted by this incident.

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; and <https://ag.ny.gov/>.

For Washington, D.C. residents: The Attorney General may be contacted at: Office of the Attorney General, 441 4th Street, NW, Washington, DC 20001; (202) 727-3400; and www.oag@dc.gov.