

Trinity Christian College  
Mail Handling Services  
777 E Park Dr  
Harrisburg, PA 17111



Dear [REDACTED]

The privacy and security of the personal information we maintain is of the utmost importance to Trinity Christian College. We are writing with important information regarding a recent data security incident at Blackbaud, a third party service provider, which may have involved some of the information that you provided to Trinity Christian College. Blackbaud is a software and service provider that is widely used for fundraising and alumni or donor engagement efforts at non-profits and universities world-wide. Trinity Christian College uses one or more Blackbaud applications, and Blackbaud recently experienced an incident impacting that application. We want to provide you with information about the incident and let you know that we continue to take significant measures to protect your information.

What Happened?

On July 16, 2020, Blackbaud notified Trinity Christian College of a security incident that impacted its clients across the world. Blackbaud reported to us that they identified an attempted ransomware attack in progress on May 20, 2020. Blackbaud informed us that they stopped the ransomware attack and engaged forensic experts to assist in their internal investigation. That investigation concluded that the threat actor intermittently removed data from Blackbaud's systems between February 7, 2020 and May 20, 2020. According to Blackbaud, they paid the threat actor to ensure that the data was permanently destroyed. On September 29, 2020, Blackbaud provided Trinity Christian College with a follow up notification regarding the incident and indicated that additional information was impacted. After undertaking a review of the additional impacted information, we determined that this information

What We Are Doing.

Upon learning of the issue, we commenced an immediate and thorough investigation. That investigation is still ongoing. As part of our investigation, in addition to demanding detailed information from Blackbaud about the nature and scope of the incident, we engaged cybersecurity professionals experienced in handling these types of incidents.

What Information Was Involved.

On January 18, 2021, following an extensive review and analysis of the data at issue, we determined that the information removed by the threat actor may have contained some of your personal information

What You Can Do.

**According to Blackbaud, there is no evidence to believe that any data will be misused, disseminated, or otherwise made publicly available. Blackbaud indicates that it has hired a third-party team of experts, including a team of forensics accountants, to continue monitoring for any such activity.** Nevertheless, out of an abundance of caution, we want to make you aware of the incident. This letter provides precautionary measures that you can take to protect your personal information, including placing a fraud alert and/or security freeze on your credit files, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis and report any suspicious activity to the proper authorities. We have also provided information on protecting your medical information on the following pages.

For More Information.

We remain fully committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. Blackbaud has assured us that they closed the vulnerability that allowed the incident and that they are enhancing their security controls and conducting ongoing efforts against incidents like this in the future. We continually evaluate and modify our practices, and those of our third party service providers, to enhance the security and privacy of your personal information.

**If you have any further questions regarding this incident, please call our toll free response line at [REDACTED]** This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available [REDACTED]  
[REDACTED]

Sincerely,

[REDACTED]

## **– OTHER IMPORTANT INFORMATION –**

### **1. Placing a Fraud Alert on Your Credit File.**

You may place an initial one (1) year “fraud alert” on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

#### **Equifax**

P.O. Box 105069  
Atlanta, GA 30348  
[www.equifax.com](http://www.equifax.com)  
1-800-525-6285

#### **Experian**

P.O. Box 2002  
Allen, TX 75013  
[www.experian.com](http://www.experian.com)  
1-888-397-3742

#### **TransUnion LLC**

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

### **2. Placing a Security Freeze on Your Credit File.**

If you are very concerned about becoming a victim of fraud or identity theft, you may request a “security freeze” be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

#### **Equifax Security Freeze**

PO Box 105788  
Atlanta, GA 30348  
<https://www.freeze.equifax.com>  
1-800-349-9960

#### **Experian Security Freeze**

PO Box 9554  
Allen, TX 75013  
<http://experian.com/freeze>  
1-888-397-3742

#### **TransUnion Security Freeze**

P.O. Box 2000  
Chester, PA 19016  
<http://www.transunion.com/securityfreeze>  
1-888-909-8872

In order to place the security freeze, 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 reporting company will send you a confirmation letter containing 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.

### **3. Obtaining a Free Credit Report.**

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

### **4. Additional Helpful Resources.**

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft), by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If this notice letter indicates that your financial account number was impacted, we recommend contacting your financial institution to inquire about ways in which you can protect your account, including getting a new account number.

**North Carolina Residents:** You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Department of Justice, 9001 Mail Service Center, Raleigh, NC 27699-9001, [www.ncdoj.gov/](http://www.ncdoj.gov/), Telephone: 877-566-7226.

## **5. Protecting Your Medical Information.**

If this notice letter indicates that your medical information was impacted, we have no information to date indicating that your medical information involved in this incident was or will be used for any unintended purposes. As a general matter, however, the following practices can help to protect you from medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.
- Review your Explanation of Benefits (EOB) which is a statement you receive from your health insurance company after you have a medical visit. Follow up with your insurance company or care provider's billing office for any items you do not recognize. If necessary, contact the care provider on the EOB statement and ask for copies of medical records from the date of the potential access (noted above) to current date at no expense to you.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.