181 81

[to be typed on Shippensburg University Foundation letterhead]

[Date], 2020

[Insert mailing address (if applicable) or email address (if applicable)]

RE: Notice of Data Breach

Dear [Name],

We are writing to let you know about a data security incident that may have involved your personal information. Shippensburg University Foundation takes the protection and proper use of your information very seriously. We are therefore contacting you to explain the incident and provide you with steps you can take to protect yourself.

What Happened?

We were recently notified by one of our third-party software and service vendors, Blackbaud, of a security incident. At this time, we understand Blackbaud discovered and stopped a ransomware attack. After discovering the attack, Blackbaud's Cyber Security team—together with independent forensics experts and law enforcement successfully prevented the cybercriminal from blocking their system access and fully encrypting files; and ultimately expelled them from their system. Prior to locking the cybercriminal out, the cybercriminal removed a copy of our backup file containing your personal information. This occurred at some point beginning on February 7, 2020 and could have been in there intermittently until May 20, 2020.

What Information Was Involved?

It is important to note that we do not have your credit card information or bank account information, therefore, the cybercriminal did not have access to this type information. However, we have determined that the file removed may have contained your social security number, along with your contact information.

Because protecting customers' data is their top priority, Blackbaud paid the cybercriminal's demand with confirmation that the copy they removed had been destroyed.

Based on Blackbaud's representations to us, including the nature of the incident, their research, and third party (including law enforcement) investigation, we have no reason to believe that any data went beyond the cybercriminal, was or will be misused, or will be disseminated or otherwise made available publicly.

What We Are Doing?

We are notifying you so that you can take immediate action to protect yourself. Ensuring the safety of our constituents' data is of the utmost importance to us. As part of their ongoing efforts to help prevent something like this from happening in the future, Blackbaud has already implemented several changes that will protect your data from any subsequent incidents.

First, Blackbaud's teams were able to quickly identify the vulnerability associated with this incident, including the tactics used by the cybercriminal, and took swift action to fix it. They have represented to us that they have confirmed through testing by multiple third parties, including the appropriate platform vendors, that their fix withstands all known attack tactics. Additionally, they are accelerating their efforts to further harden their environment through enhancements to access management, network segmentation, deployment of additional endpoint and network-based platforms.

What You Can Do?

As a best practice, we recommend you remain vigilant and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities and credit reporting agencies. For instance, you may want to consider taking some or all of the steps described on the next page – see page titled **"STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION."**

Do You Need More Information?

We sincerely apologize for this incident and regret any inconvenience it may cause you. Should you have any further questions or concerns regarding this matter and/or the protections available to you, please do not hesitate to contact [SUF's Contact Name] at [Contact Phone Number] or [Contact Email].

Sincerely,
[Name]
[Title]
Shippensburg University Foundation
1871 Old Main Drive
Shippensburg, PA 17257

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity

As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, including your state attorney general and the Federal Trade Commission (FTC).

To file a complaint with the FTC, go to www.IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

Obtain and Monitor Your Credit Report

We recommend that you obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can access the request form at: https://www.annualcreditreport.com/requestReport/requestForm.action

Or you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Equifax	Experian	TransUnion
(866) 349-5191	(888) 397-3742	(800) 888-4213
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241	P.O. Box 2002	2 Baldwin Place
Atlanta, GA 30374	Allen, TX 75013	P.O. Box 1000
		Chester, PA 19016

Consider Placing a Fraud Alert on Your Credit Report

You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com .

Take Advantage of Additional Free Resources on Identity Theft

We recommend that you review the tips provided by the Federal Trade Commission's Consumer Information website, a valuable resource with some helpful tips on how to protect your information. Additional information is available at https://www.consumer.ftc.gov/topics/privacy-identity-online-security. For more information, please visit www.IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338).

Security Freeze

In some US states, you have the right to put a security freeze on your credit file. A security freeze (also known as a credit freeze) makes it harder for someone to open a new account in your name. It is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to apply for a new credit card, wireless phone, or any service that requires a credit check. You must separately place a security freeze on your credit file with each credit reporting agency. To place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement, or insurance statement. There is no charge to request a security freeze or to remove a security freeze.

Maryland residents may also wish to review information provided by the Maryland Attorney General on how to avoid identity theft at http://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx, or by sending an email to idtheft@oag.state.md.us, or calling 410-576-6491.

Rhode Island residents may request additional information by contacting the Rhode Island, Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, (401) 274-4400.

North Carolina residents may obtain information about steps you can take to prevent identity theft from the North Carolina Attorney General at https://ncdoj.gov/protecting-consumers/protecting-your-identity/protect-yourself-from-id-theft/ or at:

North Carolina Attorney General's Office
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
877-566-7226 (Toll-free within North Carolina)
919-716-6000