GEORGIA SOUTHERN UNIVERSITY

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Notice of Data Breach

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

At Georgia Southern University, we understand the importance of protecting and securing the personal information we maintain. We are writing to notify you of a security incident experienced by one of our vendors, Blackbaud. This notice explains the incident, measures we and Blackbaud have taken, and some steps you can take in response.

What Happened?
Blackbaud is a cloud-based software company that provides services to thousands of schools, hospitals, and other non-profits. On July 16, 2020, Blackbaud notified us that it had discovered an attempted ransomware attack on Blackbaud's network in May 2020. Blackbaud reported that it conducted an investigation, determined that backup files containing information from its clients had been taken from its network, and an attempt was made to encrypt files to convince Blackbaud to pay a ransom. Blackbaud paid a ransom and obtained confirmation that the files removed from its systems had been destroyed. The time period of unauthorized access was between February 7 to May 20, 2020. Blackbaud reported that it has been working with law enforcement.

Upon learning of the incident from Blackbaud, we conducted our own investigation of the Blackbaud services we use and the information provided by Blackbaud to determine what information was involved in the incident. On September 8, 2020, we determined that the backup files contained certain information pertaining to you.

What Information Was Involved?
The backup file involved contained your name, Social Security number, and donor profile in fields that may have been viewable to the unauthorized person. Blackbaud has assured us that the backup file has been destroyed by the unauthorized individual and there is no reason to believe any data was or will be misused or will be disseminated or otherwise made available publicly.

What You Can Do.
Even though we have no evidence that your personal information has been misused, we wanted to let you know this happened and assure you we take it very seriously. We encourage you to remain vigilant by reviewing your account statements and credit reports for any unauthorized activity, as well reviewing the additional information provided in the following pages. As an added precaution, we have also secured the services of Kroll to provide identity monitoring services at no cost to you for one year. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration. For more information on your services and complimentary one-year membership, please see the additional information provided in this letter.

Visit **https://enroll.idheadquarters.com** to activate and take advantage of your identity monitoring services.
*You have until **January 13, 2021** to activate your identity monitoring services.*
Membership Number: **<<Member ID>>**

What We Are Doing.
Blackbaud has assured us that the backup file has been destroyed by the unauthorized individual and there is no reason to believe any data was or will be disseminated, misused or otherwise made available publicly. Blackbaud informed us

that they identified and fixed the vulnerability associated with this incident, implemented several changes that will better protect your data from any subsequent incidents, and are undertaking additional efforts to harden their environment through enhancements to access management, network segmentation, and deployment of additional endpoint and network-based platforms. In response to this incident, Georgia Southern University is removing all Social Security numbers from the Blackbaud database. The University is also taking additional steps with Blackbaud to better ensure that any sensitive or personal information is encrypted.

For More Information.

Your confidence and trust are important to us, and we regret any inconvenience or concern this incident may cause. Should you have any further questions or concerns regarding this matter, please call 1-866-461-1556, Monday through Friday from 8:00 A.M. through 5:30 P.M. Central Time.

Sincerely,

Trip C. Addison
Vice President for University Advancement

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax,* PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian,* PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion,* PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission,* Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

Kroll | A Division of DUFF&PHELPS

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you will have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.
To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.