Middle Georgia State University Foundation

100 University Parkway
Macon, GA 31206-5145
P 478-471-2732
F 478-471-2846
mga.edu/foundation

July 30, 2020

RE: **Notice of Data Breach**

Dear [NAME],

We were recently notified by our data management software vendor, Blackbaud, of a breach of their system between February and May 2020 and are contacting you to make you aware. Middle Georgia State University Foundation takes the protection and proper use of your information very seriously and is in detailed conversations with Blackbaud about this serious matter and their handling of information.

According to Blackbaud, credit card information, bank account information, or social security numbers **were not exposed**. However, the data that was accessed may include name, address, date of birth, contact information, school attended, field of study, date of graduation, giving history, and name of employer for some donors. Please see the FAQs attached for more information.

Also according to Blackbaud, their investigation concluded the accessed data **has not been** further exposed by the cybercriminal. Blackbaud reports that it has already implemented several changes to protect your data and reduce the risk of future incidents. While we continue to assess the scope of the incident, we are also reviewing our relationship with Blackbaud to ensure personal information remains secure.

We apologize for this inconvenience and continue to review the matter with Blackbaud. We may provide updated information should further developments provide information more actionable. If you have any questions or concerns please see the FAQs section below or contact me at 478-471-2732, or by email at ken.fincher@mga.edu.

Sincerely,

Ken L. Fincher

Dr. Ken L. Fincher, CFRE
Vice President and Executive Director
Middle Georgia State University Foundation

Blackbaud Data Security Incident Frequently Asked Questions (FAQs)

1. What happened?

On July 16, 2020, a third-party vendor, Blackbaud, informed the Middle Georgia State University (MGA) Foundation of a data breach which resulted in unauthorized access to certain information maintained by Blackbaud. Upon learning of this incident, MGA immediately commenced an investigation to determine what, if any, MGA Foundation data was impacted. Please know we take the incident and safeguarding the security of our donors' information very seriously. We are diligently working to determine the full nature and scope of this incident, as well as confirm whether and what Foundation data may be involved.

2. **When did the MGA Foundation discover that this happened?**

On July 16, 2020, our third-party vendor, Blackbaud, informed us of a data breach that occurred in May 2020. We immediately began an investigation to determine how this incident impacts the MGA Foundation, and our constituents.

3. **Who is Blackbaud and do they have my personal information?**

Blackbaud is a third-party service provider that offers customer relationship management and financial services tools, focusing on the non-profit sector. The MGA Foundation uses Blackbaud primarily for these services, including front-end fundraiser analytics, benchmarking, and prospect screening analytics.

4. **What information of mine was potentially accessed**?

The MGA Foundation is actively investigating what, if any, information was potentially impacted by Blackbaud's data breach. While our investigation is ongoing, to date, **Blackbaud advised that no credit card information was included in the impacted files, and that no bank account information, usernames, passwords or Social Security numbers were accessible to the unauthorized actor**. No encrypted data was compromised and personal financial data is encrypted.

The MGA Foundation understands from the information provided by Blackbaud, that certain giving records may have been included among the data potentially impacted by the recent incident. Such records could include donors' names, physical addresses, phone numbers, birthdates, and donor profile information, such as donors' real estate asset holdings, or giving history. We continue to investigate this incident and will provide additional updates as necessary.

5. **What is the MGA Foundation doing to prevent this from happening again?**

The Foundation is currently investigating the nature and scope of this incident and will work with Blackbaud to evaluate additional measures and safeguards to protect against this type of incident in the future.

6. **Why did it take so long to notify me**?

The MGA Foundation continues to seek information from Blackbaud regarding its investigation and response to this incident, including why the MGA Foundation and other customers were not

notified sooner. However, upon receiving initial notification from Blackbaud on July 16, 2020, the MGA Foundation immediately responded and launched an investigation to determine the extent to which MGA Foundation data may be impacted. We have been working in close coordination with the University System of Georgia office during this investigation and response. Our initial investigation and response efforts were required to ensure the accuracy of the information provided to you. The MGA Foundation then notified those whose information may be impacted.

7. **What should I do?**

According to Blackbaud, this event did not disclose your Social Security number or financial account details. Please do not hesitate to contact the MGA Foundation if you have a question about the legitimacy of any communication you receive from a source that appears to be the Middle Georgia State University Foundation.

While Blackbaud has stated that there is no evidence of further misuse of the information involved in this incident, you may wish to monitor financial transactions and your credit report:

For more information, please review information provided by the Federal Trade Commission at www.identitytheft.gov.

Monitoring your financial statements carefully. If you see any unauthorized or suspicious activity, promptly contact your bank, credit union, or credit card company.

Monitoring your credit reports for suspicious or unauthorized 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:

Experian
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
https://www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19106
1-800-680-7289
https://www.transunion.com

Equifax
P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008
https://www.equifax.com/personal

Placing a fraud alert on your credit file. You have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-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. Contact the three major credit bureaus directly to place a fraud alert on your credit file.

Placing a security freeze on your credit file. A security freeze 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. Contact the three major credit bureaus directly to place a security freeze on your credit file.

Contacting the Federal Trade Commission and your state Attorney General to learn more about identity theft, fraud alerts, security freezes, and other steps you can take to protect yourself. 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); TTY: 1-866-653-4261.

Report incidents of suspected or actual identity theft or fraud to law enforcement, the Federal Trade Commission, and your state Attorney General.

8. **Was law enforcement notified?**

Yes, Blackbaud reports that they notified the FBI and are cooperating with the FBI's investigation.

9**. Is Credit Monitoring being offered?**

Credit monitoring is not being offered as Blackbaud claims the data breach did not expose personal information used to commit identity theft. Futher, Blackbaud reported no evidence of misuse of the information involved.