18238

VIA: US Postal Service

First Name Last Name
Address
City, State, Zip

Re: Security Breach Notification

Dear Name,

At Georgia College & State 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.

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 and determined that backup files containing information from its clients had 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 07/28/20, we determined that the backup files contained certain information pertaining to you. Upon the initial investigation it was not determined the breach contained personal identifiable information but upon a later inspection on 08/04/20, that may not be the case. The unencrypted backup file involved in the Blackbaud incident contained your name, social security number (SSN), contact information, demographic information and a history of your relationship with the university (such as donation dates and gift amounts) in fields that may have been viewable to the unauthorized person. It's important to note that the cybercriminal did not access your credit card information or bank account information 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 as reviewing the additional information provided in the following pages. As an added protection, we have also secured the services of identityfraud.com to provide identity monitoring services at no cost to you for 42 months. Your identity monitoring services include 1,000,000 of ID insurance, ID risk score, SSN monitoring, credit card monitoring, unlimited victim assistance and fraud resolution.

Please contact me regarding the next steps and take advantage of your identity monitoring services.

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 College has taken the following steps:

- We believed all social security numbers were eliminated from our database several years ago, but unfortunately there were a very small number residing in hidden fields that we were unaware of – those have now been eliminated.
- All personal identification is now in secure fields that are designed and encrypted specifically to protect them.
- We are in the process of transferring our data from Blackbaud's cloud to the AZURE cloud to ensure the highest level of data security.

Your confidence and trust are important to us, and we regret any inconvenience or concern this may cause.

Should you have any further questions or concerns regarding this matter, please call (478) 445-5400 Monday through Friday from 8:00A.M. through 5:00P.M. EST.

Sincerely,

Monica Delisa
Vice President for University Advancement

enclosure

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 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 AVE NW, Washington, DC 20580, 1-877-ID-THEFT (1-877-438-4338), www.ftc.gov/idtheft

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud – an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have bee, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit report, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit

reporting company. For more information and instructions to place a security freeze, contact each fo the credit reporting agencies at the addresses below:

- Experian Security Freeze, PO Box 9554, Allen TX 75013, www.experian.com
- TransUnion Security Freeze, PO Box 2000, Chester, PA 19016, www.transunion.com
- Equifax Security Freeze, PO Box 105788, Atlanta, GA 30348, www.equifax.com

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 bureau will provide you with 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 life the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must life a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Additional information for residents of the following states:

Louisiana: You may contact and obtain information from your state attorney general at: Louisiana Department of Justice, Office of the Attorney General, Consumer Protection Section, 1885 North Third St., Baton Rouge, LA 70802, 1-225-326-6079 / 1-877-297-0995, https://www.ag.state.la.us/

Massachusetts: You may contact and obtain information from your state attorney general at: Office of Consumer Affairs & Business Regulation, 501 Boylston St. #5100, Boston, MA 02116, 1-617-973-8787, https://www.mass.gov/orgs/office-of-consumer-affairs-and-business-regulation

Maryland: You may contact and obtain information from your state attorney general at: Maryland Attorney General's Office, 200 St. Paul Place, Baltimore, MD 21202, 410-576-6300 / 1-888-743-0023, https://www.marylandattorneygeneral.gov/

New York: You may contact and obtain information from these state agencies: New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotection; New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov

North Carolina: You may contact and obtain information from your state attorney general at: North Carolina Attorney General's Office, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov

A Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street NW, Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited.
- You must give your consent for reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a 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.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.