BOSTON UNIVERSITY

Attorney General Bob Ferguson
Office of the Attorney General
1125 Washington Street SE
PO Box 40100
Olympia, WA 98504-0100
E-mail: securitybreach@atg.wa.gov

August 14, 2020

Re: Notice of Security Incident involving Boston University

Dear Attorney General Ferguson:

I am writing on behalf of Trustees of Boston University (the "University") to notify you of a recent security incident that affected the personal information of some Washington residents as a result of a service provider's breach. This breach also impacted the University's public radio station, WBUR, which is owned and operated by the University.

Blackbaud is a cloud-based software company that provides services to thousands of schools, hospitals, and other non-profits, including Boston University. On July 16, 2020, Blackbaud notified the University that it had discovered a ransomware attack on Blackbaud's network in May 2020. The unauthorized access to the system occurred sometime between February 7, 2020, and May 20, 2020. Blackbaud reported that it conducted an investigation and determined that backup files containing information from some of its clients had been taken from its network. Blackbaud paid a ransom and obtained confirmation from the cybercriminal that the backup files which had been removed from its network had been destroyed. Blackbaud reported that it has been working with law enforcement to investigate this incident.

The Data Event

The University has determined that the backup files which were exposed in the cyberattack contained the following personal information that could have been subject to unauthorized access: the individuals' names and full dates of birth. **The University <u>does not</u> store credit card information, financial account information, social security numbers, or passwords in this database** and that information was therefore not compromised by this incident. Blackbaud reported that it received confirmation that the backup files were destroyed by the cybercriminal and that there is no reason to believe any data was or will be misused or will be disseminated or otherwise made available publicly.

Notice to Washington Residents

The University will be providing written notice of this incident to all affected individuals for whom we have current addresses in the State of Washington, which includes 7,067 Washington residents. We expect this notice to be mailed on or about August 21, 2020. A copy of the form of notification

letter that is being sent on behalf of the University is attached; a similar letter is being sent on behalf of WBUR. Also, on or about August 8, 2020, the University provided email notification of this incident to all affected individuals in its database.

Other Steps Taken

Blackbaud has informed us that they identified and fixed the vulnerability associated with this incident, and have implemented several changes to mitigate the risk of future attacks. The University has also set up a website to provide impacted individuals with additional information about the breach and the University's data collection practices.

If you have any questions, please do not hesitate to contact me.

Sincerely,

DocuSigned by:
Martin A. Oppenheimer
842EC05B1015440...

Martin A. Oppenheimer
Associate General Counsel
Boston University
moppen@bu.edu

Enclosure

[NAME 1]
ADDRESS OF [NAME 1]
CITY, STATE, ZIP

August 21, 2020

Dear [NAME 1]:

We write to inform you that Boston University, along with many other institutions, was recently notified that one of our technology partners experienced a data security incident that may have involved the information of a number of members of the Boston University community. The University provided notice of this incident on its website on August 7, 2020. We are sending this letter as a separate notice in compliance with the requirements of Wash. Rev. Code §§ 19.255.010 (effective March 1, 2020). This notice explains the incident, measures we have taken, and additional 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, including Boston University. On July 16, 2020, Blackbaud notified us that it had discovered a ransomware attack on Blackbaud's network in May 2020. The unauthorized access to the system occurred sometime between February 7, 2020, and May 20, 2020. Blackbaud reported that it conducted an investigation, and determined that backup files containing information from some of its clients had been taken from its network. Blackbaud paid a ransom and obtained confirmation from the cybercriminal that the backup files that had been removed from its network had been destroyed. Blackbaud reported that it has been working with law enforcement to investigate this incident.

What Information Was Involved
We have determined that the backup files may have contained the following personal information: demographic data such as your name and full date of birth; contact and employment information; and information pertaining to your relationship with Boston University, including degrees granted and philanthropic giving history. **Boston University does not store credit card information, financial account information, social security numbers, or passwords in this database** and that information was therefore not compromised by this incident. Blackbaud also reported that the backup file has been destroyed by the cybercriminal and that there is no reason to believe any data was or will be misused or will be disseminated or otherwise made available publicly.

What We Are Doing
We are notifying you of this incident and sharing the steps that we, and Blackbaud, are taking in response. Blackbaud has informed us that they identified and fixed the vulnerability associated with this incident, and have implemented several changes that will better protect your data from any subsequent incidents. Boston University remains in regular contact with Blackbaud regarding the details of this incident and we will continue to monitor their response.

The University has also set up a website at **bu.edu/alumni/blackbaudnotice** to provide impacted individuals with additional information about the breach and the University's data collection practices.

Additional Steps You Can Take

We are providing you with the enclosed information about Identity Theft Protection. Although Social Security numbers and other sensitive personal information were not at risk in this incident, as a general practice, we recommend that you carefully check your credit reports for accounts you did not open or for inquiries from creditors you did not initiate. If you see anything you do not understand, contact a credit agency promptly. You should also regularly review your credit or debit card account statements to determine if there are any discrepancies or unusual activity listed. If you see something you do not recognize, immediately notify your financial institution.

For More Information

Boston University takes the protection and proper use of your information very seriously. We regret that this occurred and apologize for any inconvenience. Should you have any further questions or concerns regarding this matter, please do not hesitate to contact us at alumni@bu.edu.

Sincerely,

Karen Ann Engelbourg
Senior Vice President of Development & Alumni Relations

Tracy Schroeder
Vice President of Information Services & Technology and Chief Data Officer
Boston University

Enclosure

Information about Identity Theft Protection

Review Accounts and Credit Reports: It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for 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 agencies. To order your annual free credit report please visit **www.annualcreditreport.com** or call toll free at **1-877-322-8228**. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

You should promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding and protection against identity theft: Federal Trade Commission, Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438- 4338), www.ftc.gov/idtheft.

Security Freezes and Fraud Alerts:

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. 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.

A security freeze does not apply to a person or entity, or its affiliates, or collection agencies acting on behalf of the person or entity, with which you have an existing account that requests information in your credit report for the purposes of reviewing or collecting the account. Reviewing the account includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements. Please contact the three major credit reporting companies as specified below to find out more information about placing a security freeze on your credit report.

As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on your credit 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 7 years. You

can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies at the addresses or toll-free numbers listed at the bottom of this page.
For more information, including information about additional rights, you can visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf,https://www.consumerfinance.gov/learnmore/, or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.
You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed below.

Equifax (www.equifax.com)	Experian (www.experian.com)	TransUnion (www.transunion.com)
General Contact: P.O. Box 740241 Atlanta, GA 30374 800-685-1111 **Fraud Alerts**: P.O. Box 740256, Atlanta, GA 30374 **Credit Freezes**: P.O. Box 105788, Atlanta, GA 30348	**General Contact:** P.O. Box 2002 Allen, TX 75013 888-397-3742 **Fraud Alerts and Security Freezes:** P.O. Box 9554, Allen, TX 75013	**General Contact, Fraud Alerts and Security Freezes:** P.O. Box 2000 Chester, PA 19022 888-909-8872