OLYMPIC COLLEGE
Foundation

September 3, 2020

Sent Via US Mail and Email: securitybreach@atg.wa.gov

Attorney General Bob Ferguson
Office of the Attorney General State of Washington
1125 Washington St. SE
PO Box 40100
Olympia, WA 98504-0100

RE: Incident Notification

Dear Attorney General Ferguson:

Pursuant to RCW 42.56.590, the Olympic College Foundation (Foundation) is notifying you of a data security incident involving residents of the state of Washington.

Nature of Breach

On August 19, 2020, the Olympic College Foundation discovered that some of our data held with Blackbaud may have been involved in a ransomware security incident which was stopped. Blackbaud is one of the world's largest software providers to universities, schools, charities, and other nonprofit organizations, and provides data management services for the Olympic College Foundation.

Blackbaud reports that they paid the ransom demand and believes that copies of the stolen data were destroyed and were not, and will not be, misused. They also report that they corrected the vulnerability that led to this incident and are making changes to protect the Foundation's data from further incidents. Based on Blackbaud's public statements and our direct communications with them, there is no indication that the information has been misused.

The information involved in this incident may have included an affected individual's name, date of birth, gender, spouse's name, employment, record of giving to the Olympic College Foundation, participation in Foundation events and volunteer activities, and philanthropic interests.

OLYMPIC COLLEGE
Foundation

Number of Affected Individuals

The Olympic College Foundation identified approximately 25,583 Washington state residents whose name in conjunction with their date of birth may have been contained in the data accessed during the ransomware attack.

Steps The Olympic College Foundation Has Taken With Respect To Incident

The Olympic College Foundation immediately investigated the matter to determine what information in our records may have been impacted. On August 25, 2020, the Olympic College Foundation created a webpage with information about Blackbaud's data security incident.

The Olympic College Foundation is sending notification to the affected individuals of the possible exposure of their personal information. **Attached is a sample copy of the notice, which will be sent no later than September 4th.**

Contact Information

For further information about this notice, please contact me. My details appear below.

Sincerely,

Trevor *Trevor Ross*

Trevor Alexander Ross, J.D., LL. M.
Executive Director | Olympic College Foundation
1600 Chester Avenue, CSC 513 | Bremerton, WA 98337
360-475-7121 |tross@olympic.edu
Check out our new website! **OlympicCollegeFoundation.org**
Like & Follow Us on Facebook!

OLYMPIC COLLEGE
Foundation

OLYMPIC COLLEGE
Foundation

August 21,2020

<<first_name>> <<last_name>>
<<address_1>>
<<city>>, <<state_province>> <<postal_code>>

Re: Notice of Data Security Incident

At Olympic College, we take safeguarding the privacy and security of your personal information very seriously. That's why we're contacting you regarding a recent data security incident involving Blackbaud, Inc., the database software provider we use to maintain alumni, community member and donor information. While Blackbaud continues to assure us they don't believe your information was misused in any way, we're providing suggestions for steps you can take to help protect your personal information.

What happened? Blackbaud, one of the world's largest software providers to universities, schools, charities, and other nonprofit organizations, provides data management services for the Olympic College Foundation. On August 19, we discovered some of our data held with Blackbaud may have been involved in a security incident. We immediately contacted Blackbaud, who informed us that in May 2020 they discovered — and stopped — a ransomware attack on their computer systems. We investigated the matter to determine what information in our records may have been affected. Blackbaud reports that they paid the ransom demand and believes that copies of the stolen data were destroyed. They also report that they corrected the vulnerability that led to this incident and are making changes to protect our data from further incidents. Based on Blackbaud's public statements and our direct communications with them, there is no indication your information has been or will be misused.

What information was involved? The Olympic College Foundation **does not** maintain credit card numbers, bank account information or social security numbers in the Blackbaud database. The information involved in this incident may have included your name, contact information, date of birth, gender, spouse's name, employment, record of giving to Olympic College Foundation, participation in our events and volunteer activities, and philanthropic interests.

What are we doing? What you can do: Since learning of the incident, we've been in continuous communication with Blackbaud to understand the full scope of this matter. Although we have no indication that your information was misused, out of an abundance of caution, you should consider the recommendations on the following page regarding steps you can take to help protect your personal information.

For more information: If you have any further questions or concerns regarding this matter, please don't hesitate to call me directly at (360) 475-7121, from 8 a.m. to 5 p.m. Pacific Time, Monday through Friday (excluding major U.S. holidays). We are also maintaining a webpage that will remain updated with additional information: https://olympiccollegefoundation.org/blackbaud.

Please know that we deeply regret any worry or inconvenience this may cause you. Thank you very much for your involvement in and support of the Olympic College Foundation.

Sincerely,

Trevor A. Ross
Executive Director of the Olympic College Foundation

OLYMPIC COLLEGE
Foundation

Review Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant and review 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 should also promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission.

Credit Report Copy: You may 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 also contact one of the following three national credit reporting agencies:

Equifax
P.O. Box 105851 Atlanta,
GA 30348 1-800-525-6285
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013 1-888-397-3742
www.experian.com

TransUnion
P.O. Box 1000 Chester,
PA 19016 1-877-322-8228
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit file. An initial fraud alert is free and will stay on your credit file for at least one year. 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.

Security Freeze: In some U.S. states, you have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze 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 obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. There is no fee to place, lift or remove the security freeze. In order 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.
https://www.atg.wa.gov/security-freeze-procedures

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC or from your state Attorney General about steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state of residence.
Federal Trade Commission: 600 Pennsylvania Ave, NW, Washington, DC 20580, consumer.ftc.gov, and www.ftc.gov/idtheft, 1-877-438-4338

Your Rights under the Fair Credit Reporting Act (FCRA): These rights include knowing what is in your file; disputing incomplete or inaccurate information; and requiring consumer reporting agencies to correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf- 0096-fair-credit-reporting-act.pdf.