EDUCATIONAL FOUNDATION
TIDEWATER COMMUNITY COLLEGE

September 17, 2020

VIA ELECTRONIC MAIL

Office of the Attorney General
1125 Washington St. SE
Olympia, WA 98504
SecurityBreach@atg.wa.gov

RE: Notice of Blackbaud Security Incident

To Whom It May Concern:

Pursuant to RCWA 19.255.010(7)(a)(i)-(v), we are writing to inform your office of a security incident involving Blackbaud, Tidewater Community College Education Foundation's (TCCEF) third party cloud hosting company ("Security Incident").

The Security Incident potentially involved the personal information of 1,029 Washington State residents. TCCEF has notified Washington State residents of the breach via electronic mail. A sample copy of the security breach notification is attached hereto as **Exhibit A**.

What Happened

Blackbaud manages data for numerous universities and nonprofits worldwide including TCCEF. Blackbaud recently reported to TCCEF that in May 2020, it discovered and responded to a ransomware attack that involved unencrypted data that included TCCEF files. The incident occurred at some point beginning on February 7, 2020, and the Blackbaud system could have been intermittently compromised until May 20, 2020. Blackbaud's summary of the event is available at: http://www.blackbaud.com/securityincident.

The Security Incident was discovered and stopped by Blackbaud's Cyber Security team, and with the help of independent forensics experts and law enforcement, the cybercriminal was successfully prevented from blocking their system access and fully encrypting files. Prior to being expelled from their system, the cybercriminal removed copies of data that included a TCCEF backup file.

What Information Was Involved

Because of the nature of the Security Incident, Blackbaud has determined that the file removed may have contained demographic data and the following types of personal information: Name, Address, Date of Birth, Spouse Name, Phone Number, Email Address, last four digits of credit card number and expiration, and check numbers. Please note that the cybercriminal did **NOT** have access to more sensitive data such as complete credit card number, bank account information, social security number, usernames, or passwords stored in the database.

All such information, if present, was encrypted. Also, none of our data was lost or corrupted as a result of this incident.

What Blackbaud Has Done/Is Doing

Blackbaud has informed us that it confirmed that the copy of data that was removed was destroyed and that they quickly identified the vulnerability associated with this incident, and took swift action to fix it. Blackbaud also reports that it has a substantial cybersecurity practice with a dedicated team of professionals and that since the incident, independent reviewers have evaluated the program and determined that it exceeds benchmarks for both the financial and technology sectors. Blackbaud continues to employ industry-standard best practices, conducts ongoing risk assessments, aggressively tests the security of its solutions and continually assesses its infrastructure.

What TCCEF Has Done/Is Doing

Ensuring the safety of our constituents' data is of the utmost importance to us. Upon receipt of the information from Blackbaud, we have confirmed that the especially sensitive data of our donors is encrypted. We have also reviewed our technical safeguards and protocols to ensure personal information is safe. To further protect personal information, we will continue to work with Blackbaud to make certain it is taking all necessary steps to remediate this incident and prevent any further unauthorized access to personal information.

For More Information

Should you have any further questions or concerns regarding this matter, please do not hesitate to contact me directly at 757 822-1994 or lellerbe@tcc.edu.

.

Sincerely,

LaVerne W. Ellerbe

LaVerne Ellerbe, Interim Executive Director
TCC Educational Foundation

Enclosure
Exhibit A-TCCEF Security Breach Notification Letter

EDUCATIONAL FOUNDATION
TIDEWATER COMMUNITY COLLEGE

[Date], 2020

SUBJECT: **Notice of Security Incident Involving Your Personal Information**

Dear [Name],

We are writing to advise you regarding a security incident involving Blackbaud, Tidewater Community College Educational Foundation's (TCCEF) third party cloud hosting company ("Security Incident"). TCCEF takes the protection and proper use of your information very seriously. Therefore, we are contacting you directly to explain the incident and provide you with precautionary steps you can take to protect yourself and your information.

What Happened

Blackbaud manages data for numerous universities and nonprofits worldwide including TCCEF. Blackbaud recently reported to TCCEF that in May 2020, it discovered and responded to a ransomware attack that involved unencrypted data that included TCCEF files. The incident occurred at some point beginning on February 7, 2020, and the Blackbaud system could have been intermittently compromised until May 20, 2020. Blackbaud's summary of the event is available at: http://www.blackbaud.com/securityincident.

The Security Incident was discovered and stopped by Blackbaud's Cyber Security team, and with the help of independent forensics experts and law enforcement, the cybercriminal was successfully prevented from blocking their system access and fully encrypting files. Prior to being expelled from their system, the cybercriminal removed copies of data that included a TCCEF backup file.

What Information Was Involved

Because of the nature of the Security Incident, Blackbaud has determined that the file removed may have contained demographic data and the following types of your personal information: Name, Address, Date of Birth, Spouse Name, Phone Number, Email Address, last four digits of credit card number and expiration, and check numbers. Please note that the cybercriminal did NOT have access to more sensitive data including your complete credit card number, bank account information, social security number, usernames, or passwords stored in the database. All such information, if present, was encrypted. Also, none of our data was lost or corrupted as a result of this incident.

What Blackbaud Has Done/Is Doing

Blackbaud has informed us that it confirmed that the copy of data that was removed was destroyed and that they quickly identified the vulnerability associated with this incident, and took swift action to fix it. Blackbaud also reports that it has a substantial cybersecurity practice with a dedicated team of professionals and that since the incident, independent reviewers have evaluated the program and determined that it exceeds benchmarks for both the financial and technology sectors. Blackbaud continues to employ industry-standard best practices, conducts ongoing risk assessments, aggressively tests the security of its solutions and continually assesses its infrastructure.

What We Are Doing

121 College Place | Norfolk, VA 23510 757-822-1080 757-822-1975 foundation@tcc.edu advancement.tcc.edu

Ensuring the safety of our constituents' data is of the utmost importance to us. Upon receipt of the information from Blackbaud, we have confirmed that the especially sensitive data of our donors is encrypted. We have also reviewed our technical safeguards and protocols to ensure your information is safe. To further protect your information, we will continue to work with Blackbaud to make certain it is taking all necessary steps to remediate this incident and prevent any further unauthorized access to personal information.

What You Can Do

We are notifying you so that you can take immediate action to protect yourself. As a best practice, we recommend that you remain vigilant, review your accounts and promptly report any suspicious activity or suspected identity theft to the proper credit reporting agencies and or law enforcement authorities. You may also obtain additional information from these sources about preventing identity theft.

National Credit Reporting Agencies:

Order your free credit report. You may also 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

FTC and State Resources: In addition, you may 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. 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.

Washington State – Attorney General Bob Ferguson, 1125 Washington Street SE, PO Box 40100, Olympia, WA 98504-0100, Phone: (360) 753-6200, Website: https://www.atg.wa.gov/.

For More Information

Blackbaud and TCCEF sincerely apologize for this incident and regret any inconvenience it may cause you. Should you have any further questions or concerns regarding this matter and/or the protections available to you, please do not hesitate to contact TCC Educational Foundation at (757) 822-1080 or Foundation@tcc.edu.

Sincerely,

LaVerne Ellerbe, Interim Executive Director
TCC Educational Foundation