BAKER DONELSON
BEARMAN, CALDWELL & BERKOWITZ, PC

CHASE NORTH TOWER
450 LAUREL STREET
21ST FLOOR
BATON ROUGE, LOUISIANA
70801

PHONE: 225.381.7000
FAX: 225.343.3612

www.bakerdonelson.com

LAYNA S. COOK RUSH, SHAREHOLDER
Direct Dial: 225.381.7043
Direct Fax: 225.382.0243
E-Mail Address: lrush@bakerdonelson.com

August 18, 2020

Via Email

Attorney General Bob Ferguson
Washington State Office of the Attorney General
1125 Washington Street SE
PO Box 40100
Olympia, WA 98054-0100SecurityBreach@atg.wa.gov

Re: Third Party Vendor Data Incident.

Dear Attorney General Ferguson:

Please be advised that the undersigned and the law firm of Baker, Donelson, Berman, Caldwell & Berkowitz, PC represents the University of South Carolina and its affiliated foundations ("UofSC") with regard to a data incident reported by one of UofSC's third party vendors that may have impacted personal information for some Washington residents.[1] UofSC received notification from Blackbaud, Inc. ("Blackbaud") on July 16, 2020 that Blackbaud discovered and stopped a ransomware attack of Blackbaud's self-hosted platform in May 2020. Blackbaud is the global market leader in third-party donor applications used by many charities, health and educational organizations in the U.S. and abroad.

According to Blackbaud, prior to being locked out, the cybercriminals removed a copy of sensitive data from its self-hosted environment which contained information related to individuals affiliated with multiple charitable institutions. Blackbaud reports that it paid the cybercriminals' demand and received confirmation that the copy of the data removed has been destroyed. According to Blackbaud, this incident occurred at some point between February 7, 2020 and May 20, 2020 and was discovered in May of 2020.

[1] By providing this notice, UofSC does not waive any rights or defenses regarding the applicability of your State's law, the applicability of your State's data event notification statute, or personal jurisdiction.

Based upon UofSC's review of the information related to the incident that was provided by Blackbaud and review of UofSC's information hosted by Blackbaud, the subset of data that was removed may have contained names and contact information, along with some demographic information, date of birth and giving profiles and history for some UofSC constituents. UofSC has determined that 1165 Washington residents may have been impacted by this incident. Contemporaneous with this notification, UofSC is sending written notice to those Washington residents.

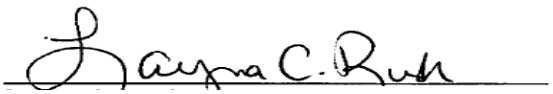
Blackbaud has stated that based on the nature of the incident, its research and third-party investigation, including investigation by law enforcement, it has no reason to believe that any data went beyond the cybercriminals, was or will be misused, or will be disseminated or otherwise made available publicly. Blackbaud reports it has hired a third-party team of experts to monitor the dark web as an extra precautionary measure. Blackbaud has also stated that it has implemented several changes to protect against subsequent incidents. Blackbaud reported it has identified the vulnerability that was associated with this incident, including the tactics used by the cybercriminal, and has taken actions to fix it. Blackbaud has asserted that it has confirmed, through testing by multiple third parties, including the appropriate platform vendors, that this fix withstands all known attack tactics. Additionally, Blackbaud has disclosed that it is accelerating its efforts to further harden its environment through enhancements to access management, network segmentation and deployment of additional endpoint and network-based platforms.

UofSC is continuing to monitor the situation, including Blackbaud's response and mitigation efforts and will provide relevant updates to its constituents as appropriate.

For more information regarding this incident, please see the template notification letter included herewith. Should you have any questions regarding the foregoing or need more information, please contact the undersigned.

Sincerely,

BAKER, DONELSON, BEARMAN,
CALDWELL & BERKOWITZ, PC

By: 
Layna C. Rush

LCR:krc
Enclosure (Notification Letter)

UNIVERSITY OF
South Carolina

University Development

August 14, 2020

To our Alumni and Friends:

This communication is to notify constituents of the University of South Carolina that Blackbaud, Inc., one of our outside vendors, recently made us aware of a data security incident that may have affected some of your personal data. UofSC and its affiliate foundations take the protection and proper use of personal data very seriously. We are, therefore, contacting you to explain the incident and the steps that have been taken in response.

What Happened?
We were recently notified by Blackbaud, Inc., that it discovered and stopped a ransomware attack on Blackbaud's infrastructure. Blackbaud is a software company that provides data services to nonprofit organizations across the country and globe. Blackbaud reports that, after discovering the attack, its cybersecurity team worked with independent forensics experts and law enforcement to expel the attacker from its system.

According to Blackbaud, prior to being locked out, the cybercriminal removed a copy of a subset of data from Blackbaud's self-hosted environment that contained information related to individuals affiliated with multiple charitable institutions. Blackbaud reports that it paid the cybercriminal's demand and received confirmation that the data copy has been destroyed. According to Blackbaud, this incident occurred at some point between February 7, 2020, and May 20, 2020, and was discovered in May 2020.

What Information Was Involved?
The subset of data that was removed may have contained constituents' names and contact information, along with some demographic information, date of birth and constituents' giving profiles and history. Based on the nature of the incident, Blackbaud's research, and third-party investigation, including law enforcement, Blackbaud has stated it has no reason to believe that any data went beyond the cybercriminal, was or will be misused, or will be disseminated or otherwise made available publicly. As an extra precautionary measure, Blackbaud reports it has hired a third-party team of experts to monitor the dark web.

What Additional Safety Measures Are Being Taken?
UofSC is continuing to monitor the situation, including Blackbaud's response and mitigation efforts. To ensure the future safety of constituents' data, Blackbaud has stated that it has implemented several changes to protect against subsequent incidents. Blackbaud reported it has

identified the vulnerability that was associated with this incident, including the tactics used by the cybercriminal, and has taken actions to fix it. Blackbaud has asserted that it has confirmed, through testing by multiple third parties, including the appropriate platform vendors, that this fix withstands all known attack tactics. Additionally, Blackbaud has disclosed that it is accelerating its efforts to further harden its environment through enhancements to access management, network segmentation and deployment of additional endpoint and network-based platforms. For additional information about Blackbaud security and response to this incident, visit https://www.blackbaud.com/securityincident. As UofSC continues to monitor this situation, we will notify our constituents directly if we obtain evidence that their personal information was exposed beyond what was described above.

What Should You Do?

It is always best practice to monitor your personal accounts and credit history for unusual activity and to contact the appropriate financial institutions, law enforcement authorities, or credit bureaus if you have concerns. Always remain alert to email and telephone scams asking for money or personal information. For your convenience, we are providing contact information for the three major credit bureaus:

3 MAJOR CREDIT BUREAUS / CONSUMER REPORTING AGENCIES		
Equifax P.O. Box 105788 Atlanta, GA 30348 1-800-525-6285 www.equifax.com	**Experian** P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com	**TransUnion** P.O. Box 2000 Chester, PA 19022 1-800-680-7289 www.transunion.com

We sincerely apologize for this incident and regret any inconvenience it may cause you. If you have questions or concerns, please contact UofSC at blackbaudincident@mailbox.sc.edu.

Sincerely,

Will Elliott
Interim Vice President of Development