Sent Via Email at SecurityBreach@atg.wa.gov July 28, 2020

Attorney General Bob Ferguson
Office of the Attorney General
Consumer Protection Division
1125 Washington Street SE
P.O. Box 40100
Olympia, WA 98504-0100

RE: Notice of Data Security Incident

Dear Attorney General Ferguson:

We are writing to notify you, pursuant to RCW § 19.255.010 (amended by HB 1071), of a recent data security incident of a third-party service provider employed by the French American School of Puget Sound ("FASPS"). This incident involves the personal information of approximately 3,172 members of FASPS's community who are Washington state residents. The personal information at issue may include the full name, contact information (including phone numbers, addresses, and emails), familial connections, and dates of birth of members of the FASPS community.

1. Nature of the security incident.
On July 16, 2020, we were notified by one of our third-party service providers, Blackbaud Hosting Services ("Blackbaud"), of a security attack on a file hosted by Blackbaud. Blackbaud reports that after discovering the attack in May of 2020, the Blackbaud's Cyber Security team—together with independent forensics experts and law enforcement— successfully prevented the cybercriminal from blocking their system access and fully encrypting files; and ultimately expelled them from their system. Prior to locking the cybercriminal out, the cybercriminal removed a copy of FASPS's backup file containing our community member's personal information. According to Blackbaud, this event occurred at some point beginning on February 7, 2020 and could have reoccurred intermittently until May 20, 2020. At present, there is no indication that the compromised information has been utilized by any bad actors or otherwise disseminated or misused.

2. Number affected residents and notification methodology.
Approximately 3,172 residents of Washington were affected by this incident. FASPS notified the affected Washington residents for whom we possess a viable email address on July 17, 2020 by email and notified the remaining 600 affected Washington residents via regular mail on July 24, 2020 (a copy of which is attached to this letter).

3. Steps taken in response to the incident.
As part of its mitigation efforts, Blackbaud affirms that it has implemented several changes to prevent future such incidents. According to Blackbaud, Blackbaud's teams quickly identified the vulnerability associated with this incident, including the tactics used by the cybercriminal, and took swift action to fix it. Blackbaud has confirmed through testing by multiple third parties, including the appropriate platform

vendors, that the fix withstands all known attack tactics. Additionally, Blackbaud avows that it is accelerating their efforts to further reinforce their environment through enhancements to access management, network segmentation, deployment of additional endpoint and network-based platforms.

4. Contact Information.
FASPS is committed to protecting its community's personal information that is within its control. Should you have any questions or need additional information, please do not hesitate to contact our Development Director at (206) 275-3533, ext. 278 or by email at HeidiP@FASPS.org.

Please let us know if you have any questions.

Best Regards,

Eric Thuau
Head of School
French American School of Puget Sound

Attachment 1: Notification Letter to Affected FASPS Community Members
Attachment 2: Notification Letter from Blackbaud to the French American School of Puget Sound

Attachment 1

Dear <Name>,

I wanted to let you know that we were recently informed that the provider of the software we use for contact management of our fundraising efforts, Blackbaud, suffered a ransomware attack on their servers, which may have comprised our records. Please see the information they shared below (copied and pasted from this webpage):

- *"Prior to our locking the cybercriminal out, the cybercriminal removed a copy of a subset of data from our self-hosted environment. The cybercriminal did not access credit card information, bank account information, or Social Security numbers. Because protecting our customers' data is our top priority, we paid the cybercriminal's demand with confirmation that the copy they removed had been destroyed. Based on the nature of the incident, our research, and third-party (including law enforcement) investigation, we have 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."*

We want to assure you that we do not keep credit card or bank account information in our Blackbaud software, which is called Raiser's Edge. We also do not store Social Security numbers. Our records do include names, addresses, phone numbers, and, in some records, date of birth. Records also include gift information but not the specific details of the gift (i.e., a gift paid by credit card does not include the credit card number, just date and amount of the donation). The same procedure applies to checks, gifts of stocks, and other forms of payment.

Please note, and let me repeat, the cybercriminal did NOT access your credit card information, bank account information, or Social Security number; the file removed, however, may have contained your name, contact information, and date of birth.

As a best practice, we recommend you remain vigilant and promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities. In case you would like to reach out to the three credit bureaus, following are their toll-free numbers: Equifax: 1-888-548-7878; TransUnion: 1-800-916-8800; Experian: 1-800-493-1058.

We are very sorry that this has happened and regret any inconvenience it may cause you. Should you have any further questions or concerns regarding this matter, please do not hesitate to contact Heidi Paige in the Development Office at HeidiP@FASPS.org.

Thank you for all that you do to support FASPS.

Sincere regards,

Eric Thuau
Head of School

Attachment 2

Received Via Email on July 16, 2020

Re: Notification of Security Incident

Dear [Director of IT at the French American School of Puget Sound],

We are writing to notify you about a particular security incident that recently occurred. Please review this email for a personalized link, next steps and resources created for your organization specifically.

What Happened

The Cybercrime industry represents an over trillion-dollar industry that is ever-changing and growing all the time—a threat to all companies around the world. At Blackbaud, our Cyber Security team successfully defends against millions of attacks each month and is constantly studying the landscape to ensure we are able to stay ahead of this sophisticated criminal industry. **In May of 2020, we discovered and stopped a ransomware attack. In a ransomware attack, cybercriminals attempt to disrupt the business by locking companies out of their own data and servers. After discovering the attempted attack, our Cyber Security team—together with independent forensics experts and law enforcement—successfully prevented the cybercriminal from blocking our system access and fully encrypting files; and ultimately expelled them from our system.**

Prior to our locking the cybercriminal out, the cybercriminal removed a copy of a subset of data from our self-hosted environment. The cybercriminal did not access credit card information, bank account information, or social security numbers. Because protecting our customers' data was our top priority, we paid the cybercriminal's demand with confirmation that the copy they removed had been destroyed.

Based on the nature of the incident, our research, and third party (including law enforcement) investigation, we have 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. In accordance with regulatory requirements and in an abundance of caution, we are notifying all organizations whose data was part of this incident and are providing resources and tools to help them assess this incident.

What This Means for Your Organization Specifically

Our public cloud environment (Microsoft Azure and Amazon Web Services) and most of our self-hosted datacenters, products and customers were not part of this incident, but we have confirmed the following specific to your organization:

- A copy of your Blackbaud Raiser's Edge NXT and ResearchPoint backup was part of this incident. Again, the file the cybercriminal removed a copy of did not contain any credit card information. Further, the cybercriminal did not gain access to bank account information, usernames, passwords, or social security numbers stored in your database because they were encrypted. None of your data was lost or corrupted as a result of this incident.

And again, based on the nature of the incident, our research, and third party (including law enforcement) investigation, we have 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. We have hired a third-party team of experts to monitor the dark web as an extra precautionary measure.

We have created a resource page for you at www.blackbaud.com/incidentresources that features a toolkit with a step-by-step guide to help you as you digest this information. It also contains answers to key questions, links to educational webinars (hosted by Rich Friedberg, Blackbaud's Chief Information Security Officer and Cameron Stoll, our Head of Privacy), information about our future plans, and other resources.

It is unlikely but possible, depending on jurisdiction, that our customers may have to make further notifications to constituents or other third parties. Your toolkit provides a written guide to notification laws and access to a webinar that helps you assess potential notification requirements in your jurisdictions. We advise you to also consult with your organization's legal counsel to understand any notification requirements. We want to continue to be your partner through this incident. If you determine that you do need to notify your constituents, we have included templates in your toolkit to make it easier.

To ensure all your questions are answered as quickly as possible, we encourage you to first review the resources we provided at the link above. If you still have questions after reviewing these resources, we are here to help. Please contact the dedicated team we have established for this incident:

- **North and South America:** 1-855-907-2099 between 9 a.m. and 9 p.m. ET Monday – Friday

We understand this situation is frustrating. This was a very sophisticated attack, and while we were able to defend against it for the most part, we realize this is still requiring that you invest time to review the situation, and that you may need to invest time to take follow-up actions. We apologize for this and will continue to do our very best to supply help and support as we and our customers jointly navigate any necessary response to the cybercriminal's actions.

Sincerely,

Todd Lant
Chief Information Officer

blackbaud