August 27, 2020

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

Attorney General Ferguson:

This letter is to inform you of a recent security incident that affected the personal information of Washington state residents.

The Security Event: Time Frame and Personal Information Involved
The University of Puget Sound was notified on July 16, 2020 of a data security incident experienced by our third-party vendor, Blackbaud, that occurred in May 2020. Blackbaud is a customer relationship management system that the university utilizes for donor prospect research. During a ransomware attack launched at Blackbaud, copies of customer data, including data from the University of Puget Sound, were acquired by the cybercriminals. Blackbaud believes that all copies of the acquired data were destroyed after they had paid a ransom and are monitoring for data exposure. For Blackbaud's statement on the incident, see https://www.blackbaud.com/securityincident.

Upon notice of the event, the University of Puget Sound responded by immediately initiating its own investigation into the incident. From the internal examination conducted, we determined that the data which may have been subject to unauthorized access included personal information as defined in RCW 19.255.0.010, specifically, full name, address, and date of birth. We identified the individuals whose records in our electronic file contained date of birth in combination with name, consistent with the statutory requirements.

Notice to Washington Residents
On August 24th, the University of Puget Sound provided notice via electronic mail to those affected individuals, which included approximately 1,429 Washington state residents. A copy of the notice is attached. The delay in messaging was due to necessary measures to determine the scope of the breach and correctly identify affected constituents.

Steps Taken To Contain Breach and Other Steps Taken
While the University of Puget Sound was not the target of this attack, nor was it the only organization affected, we are taking the following steps as a result of this third-party incident: we are reviewing internal security practices and system configurations to even better protect personal information in the future, we are working to improve our review process for approving third-party cloud solutions, and we have followed up with Blackbaud to confirm their actions going forward to limit future breaches. Blackbaud has assured us that the vulnerability leading to this incident was fixed and that additional steps are being taken to protect against future cyberattacks by hardening systems and performing regular security audits.

Should you have any questions regarding this notification or other aspects of the data security event, please contact the undersigned at (253) 879-2734.

Sincerely,

Joanna Carey Cleveland
Vice President and University Counsel

Enclosure

Dear [Constituent First Name],

I am writing to inform you of a data security incident experienced by Blackbaud, Inc., one of the University of Puget Sound's third-party service providers, and one of the world's largest providers of customer relationship management software. A portion of your information on file with the university – not including social security numbers, bank account information, passwords, or credit and debit card information – was involved in a recent ransomware attack targeting Blackbaud. The company has assured us that no encrypted data was accessible; however, even though there is no indication that your information was or will be misused in any way, we want to provide you with information about the incident and the steps being taken to mitigate any adverse effects that might result.

On July 16, 2020, Blackbaud notified the University of Puget Sound that Blackbaud's system had been the target of a ransomware attack and that a number of the university's constituent relations files may have been compromised. Blackbaud further reported that they discovered the incident in May 2020. To protect the data and prevent its misuse by cybercriminals, Blackbaud paid a ransom and consequently received confirmation that the cybercriminals destroyed all copies of the stolen data. Based on prior incidents similar to this and independent third-party investigations that included law enforcement, Blackbaud notified us and other affected businesses and organizations that they have no reason to believe any data went beyond the cybercriminals; that any data was or will be misused; or that any data will be disseminated or otherwise made available publicly. Further, third-party teams of cybersecurity experts are continuing to monitor for any indications of data exposure on the dark web. For Blackbaud's statement on the incident, see https://www.blackbaud.com/securityincident.

Upon receiving notification from Blackbaud of this incident, the university immediately initiated its own investigation to better understand how our alumni, parents, and friends might have been affected. From our internal investigation, we determined that an electronic file containing certain constituent and prospective constituent records may have been involved. Most of the affected data fields in the compromised file contained non-sensitive publicly available information such as name, property address, and/or spouse's name. However, the compromised file also included a data field containing full date of birth. First and last name in combination with full date of birth is protected personal information under Washington law.

While it appears that the breach of the security of Blackbaud's system is not reasonably likely to subject you to a risk of harm, now that we have completed our investigation we nonetheless think it is important to notify you of this incident so you can remain vigilant for any possible suspicious activity. We want to emphasize again that Blackbaud did not have in its possession your credit or debit card information, bank account information, passwords, or social security number.

We do not believe there is a need for our constituents to take any action at this time. If you desire to take proactive steps to protect your information out of an abundance of caution, you may review your credit reports, set up a security freeze, or set up fraud alerts. Those actions can be performed through any one of the major credit-reporting bureaus:

◊ Equifax 1-800-525-6285
◊ Experian 1-888-397-3742
◊ Trans Union 1-800-680-7289

Puget Sound remains committed to the security and protection of your personal information. Blackbaud has assured us that they fixed the vulnerability leading to this incident and is taking additional steps to protect against future cyberattacks. While Puget Sound was not the target of this attack, nor was it the only organization affected, we are taking time to learn from this third- party incident and review our own security practices and system configurations to even better protect your information. We are also examining, specifically, our relationship with Blackbaud in light of this incident.

We deeply regret that this incident occurred through one of our trusted vendors and regret any inconvenience it may cause you. If you have further questions, you may contact us at vpour@pugetsound.edu or 253-879-3622.

Sincerely,

Dave Beers

David R. Beers P'11 | Vice President for University Relations

UNIVERSITY OF PUGET SOUND

1500 N. Warner St. #1085
Tacoma, WA 98416-1085
253.879.3901
pugetsound.edu