Dear member of the Wolves family,

I am writing to let you know about a data security incident involving one of our service providers that may have included some of your personal information. This incident **did not** involve access to payment card data, bank account information or social security numbers.

What happened

One of our third-party service providers, Blackbaud, experienced a ransomware attack. Blackbaud is one of the world's largest providers of customer relationship management and financial systems for nonprofit organizations and the higher education sector. After discovering the attack, the company's cyber security team—together with independent forensics experts and law enforcement—successfully prevented the cybercriminal from blocking access to Blackbaud's system and fully encrypting files, ultimately expelling the cybercriminal from its system.

Before locking the cybercriminal out, the cybercriminal removed a copy of a backup file containing personal information from a number of Blackbaud's clients. Blackbaud confirms that to protect constituent data and mitigate potential identity theft, it met the cybercriminal's ransomware demand, paid the ransom, and received assurances from the cybercriminal and third-party experts that the data was destroyed. Blackbaud has been and will continue to monitor the web in an effort to verify the data accessed by the cybercriminal has not been misused.

What information was involved

The file that was removed may have contained your contact details, demographic information and a history of your relationship with WOU Foundation, such as donation dates and amounts and associated paperwork/correspondence. To reiterate: The cybercriminal **did not** access your credit card information, bank account information or social security number.

What happens now

In an effort to be transparent, we are making you aware of this incident. As part of its ongoing efforts to help prevent future incidents, Blackbaud has already implemented several changes to its data-protection system.

Although no payment card or bank account information is believed to have been compromised, as a best practice Blackbaud and WOU Foundation recommend

you promptly report any suspicious activity or suspected identity theft to authorities such as the Federal Trade Commission, and the Office of the Oregon State Attorney General as well as consumer reporting agencies.

We value the confidence you have placed in us and apologize for any worry or inconvenience this may cause. If you have any questions regarding this matter, please contact us. We have set up email and voicemail channels for this purpose, and we will respond to you promptly.

Email: BlackbaudBreachResponse@wou.edu

Voicemail (we will return your call promptly): **503-838-9650**

Sincerely,

Erin McDonough
Executive Director
WOU Foundation