18105

[ORGANIZATION LETTERHEAD]

[DATE]

[INDIVIDUAL NAME]
[STREET ADDRESS]
[CITY, STATE AND POSTAL CODE]
[CREDIT MONITORING PROMOTION CODE]

NOTICE OF DATA BREACH

Dear Northwest Contractor,

We are writing to inform you about a data security incident involving Blackbaud, Inc., a service provider of the Northwest Foundation. As you may be aware, Blackbaud, an engagement and fundraising software service provider, recently experienced a data breach. Northwest Foundation is one of many schools and non-profits that have been affected. The Foundation takes our relationship with you and our data protection responsibilities very seriously. You are receiving this notice in your capacity as an annuitant or vendor of the foundation. If you are also a donor, you may have already received a different notice that relates to your donor information.

Please be assured that we do not store bank account numbers and that type of information was not accessed by the cybercriminal. Blackbaud also assured us that the file accessed by the cybercriminal did not contain any credit card information and that they use encryption to store any financial account information. Further details are below, including steps we have taken in response.

What Happened

On July 16, 2020, we were contacted by Blackbaud, one of the world's largest providers of customer relationship management systems for not-for-profit organizations and the higher education sector. Company representatives informed us that a Blackbaud service provider had been the victim of a ransomware attack that culminated in May 2020. The cybercriminal was unsuccessful in blocking access to the database involved in the attack, however, the cybercriminal was able to remove a copy of a subset of data from several of Blackbaud's clients including data of Northwest Foundation.

We received a subsequent notification from Blackbaud on September 29th which informed us that Blackbaud had created a temporary file during a data conversion which included an unencrypted social security number field. While the information was accessible by the cybercriminal, there is no indication that the information was or has been misused.

What Information Was Involved

We would like to reassure our constituents that a detailed forensic investigation was undertaken, on behalf of Blackbaud, by law enforcement and third-party cyber security experts.

As noted above, Blackbaud has confirmed that the investigation found that the cybercriminal did not access your credit or debit card information, bank account information because that information was stored in an encrypted format.

Based on our own internal investigation it was discovered that several of our vendors used their social security number instead of a federal employee identification number on documentation retained by us. This information was not encrypted and may have been accessed by the cybercriminal.

Other Northwest Foundation data accessed by the cybercriminal in the Blackbaud database *may* have contained some of the following information in some of the data records if you are also a donor:

- Public information such as name, title, date of birth, spouse
- Addresses and contact details such as phone numbers and e-mail addresses
- Philanthropic interests, giving capacity and giving history to the Northwest Foundation
- Educational attainment

The student records of Northwest Missouri State University were not involved in this incident.

What Blackbaud Is Doing

We have been informed by Blackbaud that in order to protect constituent data of Blackbaud clients like Northwest Foundation and mitigate potential identity theft, it met the cybercriminal's ransomware demand. Blackbaud has advised us that it has received assurances from the cybercriminal and third-party experts that the data was destroyed and thus is no longer usable or accessible by any unauthorized persons or entities. Blackbaud informs us that it continues to monitor the web in an effort to verify the data accessed by the cybercriminal has not been misused.

Steps We Have Taken in Response

Upon notification of this breach by Blackbaud, we immediately launched our own investigation and have taken the following steps:

- We are notifying affected alumni and friends to make them aware of this breach of Blackbaud's systems;
- We are notifying any vendors and annuitants that may have been affected to make them aware of this breach of Blackbaud's systems;
- We are working with Blackbaud to understand why there was a delay between it finding the breach and notifying us, as well as what actions Blackbaud is taking to increase its security;
- We are conferring with other Blackbaud clients to share information about this breach, resulting corrective actions and identify any additional recommended best practices.

What You Can Do

We do not believe there is a need for our constituents to take any action at this time. Although your financial account information was not accessed in this security breach, below is some information about how to protect your financial information should you have other reasons to be concerned. We

recommend people remain vigilant and promptly report any suspicious account activity or suspected identity theft to the proper authorities.

- Review Your Account Statements and Notify Law Enforcement of Suspicious Activity.

As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, including your state attorney general and the Federal Trade Commission (FTC).

To file a complaint with the FTC, go to IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

- Obtain and Monitor Your Credit Report.

We recommend that you obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can access the request form at https://www.annualcreditreport.com/requestReport/requestForm.action. Or you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Equifax
(866) 349-5191
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374

Experian
(888) 397-3742
www.experian.com
P.O. Box 4500
Allen, TX 75013

TransUnion
(800) 888-4213
www.transunion.com
2 Baldwin Place
P.O. Box 1000
Chester, PA 19016

- Consider Placing a Fraud Alert on Your Credit Report.

You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity

within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

- Security Freeze.

In some US states, you have the right to put a security freeze on your credit file. A security freeze (also known as a credit freeze) makes it harder for someone to open a new account in your name. It is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to apply for a new credit card, wireless phone, or any service that requires a credit check. You must separately place a security freeze on your credit file with each credit reporting agency. To place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement, or insurance statement. There is no charge to request a security freeze or to remove a security freeze.

- Take Advantage of Additional Free Resources on Identity Theft.

We recommend that you review the tips provided by the Federal Trade Commission's Consumer Information website, a valuable resource with some helpful tips on how to protect your information. Additional information is available at https://www.consumer.ftc.gov/topics/privacy-identity-online-security.

For more information, please visit IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). A copy of Identity Theft – A Recovery Plan, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at https://www.consumer.ftc.gov/articles/pdf-0009_identitytheft_a_recovery_plan.pdf.

FOR MORE INFORMATION

For questions related to the security incident, contact Lori Steiner, Northwest Foundation Chief Finance Officer, 660-562-1411, foundation@nwmissouri.edu.

We will continue to work with Blackbaud to investigate this incident. We regret the inconvenience that this data breach may have caused. Please be assured that we take data protection very seriously and are grateful for the continued support of our alumni and friends.

Sincerely,

Dr. Bob Burrell
President, Northwest Foundation, Inc.