Blackbaud Security Incident Notification

As a valued member of our community, we want you to know about an incident that may have involved your personal information.

Blackbaud Inc, a service provider to the North Hennepin Community College Foundation, notified us that they experienced a data security incident. You may have already received notification about this incident from other nonprofits you support, as Blackbaud's fundraising and database services are used by thousands of nonprofit organizations worldwide and at 15 of the 37 institutions of higher education in the Minnesota State System.

North Hennepin Community College Foundation takes data protection responsibilities very seriously. Further details are listed below as well as the steps that you can take to protect yourself.

What's Important to Know
No credit card, bank account, or other unique and sensitive information, such as social security number, was compromised.

What Happened
Blackbaud was the target of a ransomware attack sometime between February 7, 2020 and intermittently until May 20, 2020. In a ransomware attack, cybercriminals attempt to disrupt business by locking companies out of their own data and servers. The cybercriminal was unsuccessful in blocking access to the database involved in the attack. However, the cybercriminal removed a copy of a backup file containing some personal information. According to Blackbaud, they paid the cybercriminals to ensure that the data taken was destroyed. A detailed forensic investigation was taken undertaken, on behalf of Blackbaud, by law enforcement and third-party cyber security experts.

Blackbaud informed us of this security incident on July 16, 2020. On that same day, the Minnesota State System Information Technologies and Legal team launched an independent investigation and provided us confirmation of Blackbaud's findings.

What Information Was Involved
North Hennepin Community College Foundation **does not store** any bank account, credit card, or social security numbers within the Blackbaud system. The information obtained by the cybercriminals could include name, address, phone, email, and if applicable, date of birth, and/or philanthropic giving history such as donation dates and amounts.

What Action Is Being Taken By Blackbaud?
According to Blackbaud, there is no evidence to believe that any data will be misused, disseminated, or otherwise made publicly available. Blackbaud has implemented several changes to protect data, hired a third-party team of experts, including a team of forensic accountants, to indefinitely continue monitoring for any such activity.

What We Are Doing
We sincerely apologize for this incident and regret any inconvenience it may cause. Upon learning of this issue, we commenced an immediate investigation, which is ongoing. We take data security very seriously, along with the trust you place in us. We are committed to safeguarding our donor's personal data and will continue to work with Blackbaud to ensure your privacy and security is not compromised.

What You Can Do
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 such as the Federal Trade Commission, and the Office of the Minnesota State Attorney General.

You can learn more about this incident by visiting blackbaud.com/securityincident. Should you have any further questions or concerns regarding this matter, contact Dale Fagre, NHCC Foundation Executive Director, 763-424-0909, Dale.Fagre@nhcc.edu.

We very much regret this inconvenience that this data breach may have caused. We are grateful for the continued support of our donors, alumni and community.