



October 28, 2020

RE: Notice of Data Breach

Dear Supporter,

As a valued member of the Carroll Community College community, we are writing to share with you about a data security incident that Blackbaud, Inc., our third-party customer relationship software service provider has reported to us that may have involved your personal information. Carroll Community College takes the protection and proper use of your information very seriously. We are therefore contacting you to explain the incident and provide you with steps you can take to protect yourself.

What Happened

Blackbaud recently notified us of a security incident. At this time, we understand they discovered and stopped a ransomware attack. After discovering the attack, Blackbaud's 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 our backup file containing your personal information.

What Information Was Involved

It's important to note that the cybercriminal did not access your credit card information, bank account information, or social security number. However, we have determined that the file removed may have contained your contact information, demographic information, and a history of your relationship with our organization, such as donation dates and amounts.

Because protecting customers' data is their top priority, our third-party service provider paid the cybercriminal's demand with confirmation that the copy they removed had been destroyed.

Based on the nature of the incident, their 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.

What We Are Doing

We are notifying you so that you are aware of the situation. Ensuring the safety of our constituents' data is of the utmost importance to us. As part of their ongoing efforts to help prevent something like this from happening in the future, our third-party service provider has already implemented several changes that will protect your data from any subsequent incidents.

First, the provider's teams were able to quickly identify the vulnerability associated with this incident, including the tactics used by the cybercriminal, and took swift action to fix it. We have confirmed through testing by multiple third parties, including the appropriate platform vendors, that the fix withstands all known attack tactics. Additionally, they are accelerating their efforts to further harden their environment through enhancements to access management, network segmentation, deployment of additional endpoint and network-based platforms.

What You Can Do

As a best practice, we recommend you remain vigilant and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities.

For More Information

We sincerely apologize for this incident and regret any inconvenience it may cause you. Should you have any further questions or concerns regarding this matter and/or the protections available to you, please do not hesitate to contact me via e-mail at swantz@carrollcc.edu or by phone at (410) 386-8154.

Sincerely,

A handwritten signature in blue ink that reads "Steven L. Wantz".

Steven L. Wantz
Executive Director