Blackbaud Data Breach Website FAQs

What Happened?
On July 16, 2020, we were notified by Blackbaud, Inc., one of our third-party service providers, of a security incident. At this time, we understand they discovered and stopped a ransomware attack. After discovering the attack, the service provider's Cyber 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. This occurred at some point between February 7, 2020, and May 20, 2020. Blackbaud's incident summary report is available at: https://www.blackbaud.com/securityincident.

What Information was Involved?
The cybercriminal did not access your credit card information, bank account information, or social security number during this attack. However, we have determined that the removed file may have contained your contact information, employer, date of birth, and a history of your engagement with NRCM and our fundraising activities, such as inquiries, event participation, volunteering, and donations. According to Blackbaud, they paid the cybercriminal's demand with confirmation that the copy of stolen data they removed had been destroyed. Based on the nature of the incident, their research, and third party (including law enforcement) investigation, Blackbaud has told us they 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 is NRCM Doing?
We take the data security of member information very seriously. After receiving notification of this incident, we conducted an extensive review of the information that may have been compromised during this breach. We are also undertaking an internal review to ensure all member information is always securely stored. We are notifying you so you can be on the lookout for any potential misuse of your personal information.

What is Blackbaud Doing?
As part of their ongoing efforts to prevent something like this from happening in the future, Blackbaud is accelerating efforts to further harden their environment through enhancements to access management, network segmentation, and deployment of additional endpoint and network-based platforms.

What Can I 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. You may also wish to consult the Identity Theft & Privacy resources available through the Office of the Attorney General for your state.

For More Information
We deeply value your relationship with NRCM and assure you that we take the protection of member information very seriously. Should you have any further questions or concerns regarding this matter, please contact datasecurity@nrcm.org.

Updated: 8/16/2020