October 20, 2020

We are reaching out to our donor community to let you know about a data security incident at one of our technology service providers, Blackbaud, which may have involved your personal information. Blackbaud is one of the world's largest providers of customer relationship management software. While Camp Korey is one of many organizations to be affected by this incident, we would like you to be aware of the situation and understand how you may protect yourself from any potential misuse of your information.

What happened?
Blackbaud has disclosed that it was the victim of an attempted ransomware attack. Although Blackbaud ultimately thwarted the attack, the perpetrator first copied a subset of data. While we continue to be in contact with Blackbaud to understand the breadth of this incident, investigation, and next steps, we have been assured by Blackbaud that the stolen data has been destroyed and there is no reason to believe the data was or will be misused, or will be disseminated or otherwise made available publicly. As is the case with any cybercrime, it cannot be ruled out that your personal information may have been subject to unauthorized access.

Out of an abundance of care and caution, we wanted to make you aware of this unfortunate situation. Blackbaud is a premier cloud computing provider for over 45,000 non-profits around the world and Camp Korey is just one of many of their clients affected by this attack. Therefore, you may have received or will receive notification from other organizations regarding this matter. Please note that each organization's situation is unique based on the type of Blackbaud products they use and potential data exposure.

What information was involved?
Based on review of the database, we have reason to believe that it contained some of our donors' information, including names and contact information – specifically email address and telephone number. Importantly, Blackbaud informed us that bank account and credit card account information were encrypted, and therefore not able to be accessed by the unauthorized individual.

Blackbaud has already implemented changes to its security controls to better protect against a potential future attack, and we are working with Blackbaud and other resources to assess the best path forward. We are committed to data privacy and security at all levels and we are reviewing our own security practices and systems to ensure proper protection of your information.

What can you do?
Remain vigilant about unexpected requests or communications that purport to come from Camp Korey. Compare contact information in suspicious communications with official Camp Korey contact information on our website and in other communications known to have come from us. Report suspicious activity to us or to law enforcement.

For your own purpose and understanding, know that when we solicit donations, we ask that they be submitted through our official website portal on our official web domain: campkorey.org. We will never ask for your Social Security Number or other sensitive information unrelated or unnecessary to the donation process or to purchase gift cards or other goods on our behalf.

Need more information?
We remain committed to protecting your personal information and we are grateful for your trust. We regret any inconvenience this incident may cause. To learn more about this incident, see Blackbaud's statement at https://www.blackbaud.com/securityincident. If you have questions for us, please contact info@campkorey.org or call 425-440-0850.

Sincerely,

J. Henningsen

Jay Henningsen
CEO Camp Korey