Volunteers of America®
MINNESOTA AND WISCONSIN

Notice of Data Breach

What Happened

We were recently notified by one of our third-party service providers, Blackbaud, of a security incident. Blackbaud—a company that provides us data management and software services—provides services to nonprofits all over the world, and so you may be seeing similar notices from other organizations where you have made financial contributions in the past. 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 donors' personal information. This occurred at some point beginning on February 7, 2020 and could have been in there intermittently until May 20, 2020.

What Information Was Involved

It is important to note that the cybercriminal **did not access donor credit card information, bank account information, or social security numbers**. However, we have determined that the file removed may have contained donor contact information, demographic information, and a history of donor relationships 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, Blackbaud's 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 believe that Blackbaud responded to this incident and have determined that this incident is not reasonably likely to subject you/donors to a risk of harm. We are notifying you so that donors can take immediate action to protect themselves. 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 donor data from any subsequent incidents. Blackbaud'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. They have confirmed through testing by multiple third parties, including the appropriate platform vendors, that its fix withstands all known attack tactics. Additionally, Blackbaud is accelerating its efforts to further harden its environment through enhancements to access management, network segmentation, deployment of additional endpoint and network-based platforms.

Volunteers of America Minnesota and Wisconsin has also taken appropriate internal measures related to our use of Blackbaud's services and will continue to assess our ongoing relationship with Blackbaud.

What You Can Do

No financial information was involved, and we believe the data was destroyed, and so we do not believe that this incident creates a risk of harm to our donors and volunteers. As always, you should remain vigilant and use best practices to prevent identify theft, including using complex and unique passwords online, and be on the lookout for email scams. You can learn more from Minnesota's Attorney General at: https://www.ag.state.mn.us/Consumer/Publications/IdentityTheft.asp.

For More Information

We at Volunteers of America Minnesota and Wisconsin appreciate your trust, and regret this has occurred. **We take your privacy very seriously, and we will continue to work diligently to protect your personal information.**

If you have any questions, please reach out to Volunteers of America Minnesota and Wisconsin at info@voamn.org.