The VFW Foundation was informed of a data security incident experienced by one of our trusted vendors, Blackbaud Inc., that impacted our donor database and may have involved personal information about supporters. Blackbaud is a well-respected provider of cloud and data services used by more than 25,000 organizations in more than 60 countries. VFW Foundation uses Blackbaud's fundraising technology platform.

Blackbaud discovered a ransomware attack in May of 2020 that included information in donor databases of many nonprofits organizations, including ours. The company took time to determine which organizations were impacted. Blackbaud stated that its Cyber Security team — together with independent forensics experts and law enforcement — successfully prevented the cybercriminal from blocking Blackbaud's system access. Blackbaud ultimately expelled the cybercriminal from its system. Prior to locking the cybercriminal out, however, the cybercriminal removed a copy of a backup file. (Read Blackbaud's statement about the incident.)

What information was involved

Blackbaud has assured us that credit card information and banking information were not accessed by the cybercriminal and remained encrypted. However, Blackbaud determined that the information removed and presumably destroyed may have included: names; contact information, including telephone numbers, email addresses, and mailing addresses; and a history of donor relationships with our organization, such as donation dates, amounts, and other information in donor profiles.

To protect personal customer data, Blackbaud paid the cybercriminal's demand with confirmation that the removed copy had been destroyed. Based on the nature of the incident, Blackbaud's research, and third party (including law enforcement) investigation, Blackbaud does not believe any data went beyond the cybercriminal, was or will be misused, or will be disseminated or otherwise made available publicly.

What Blackbaud is doing

As part of ongoing efforts, Blackbaud states that it already has implemented several changes that will protect your data from any subsequent incidents. First, its teams identified the vulnerability associated with this incident, including the tactics used by the cybercriminal, and took action to fix it. Blackbaud has tested its fix with multiple third parties, including the appropriate platform vendors, and assured us that it withstands all known attack tactics. They also are accelerating their efforts to further protect data through enhancements to access management, network segmentation, deployment of additional endpoint, and network-based platforms.

What you can do

We want to emphasize again that Blackbaud has assured us that no credit card, bank account, or other information of that nature was compromised. However, as a best practice, we recommend that supporters remain vigilant by reviewing their account statements and credit reports closely and reporting any suspicious activities.

- If you receive unsolicited requests for donations from us or other nonprofits, then call the number on the organization's website to confirm the legitimacy of the solicitation.
- You can obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com, calling toll-free 877-322-8228, or completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348.
- If you detect any suspicious activity, then promptly notify the financial institution or company where the account is maintained. You also should report any fraudulent activity or suspected incidence of identity theft to law enforcement authorities, your state attorney general, and/or the Federal Trade Commission.
- To file a complaint with the FTC, go to www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338). The Federal Trade Commission offers tips on how to avoid identity theft. For more information, please visit http://www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338).

VFW Foundation's commitment

While data breaches and ransomware attacks are becoming more common, this is not something VFW Foundation ever wants to happen to our valued supporters. The privacy of our supporters is of utmost importance to us. We deeply regret this incident occurred and regret any inconvenience it may cause you.

If you have any questions or concerns regarding this matter, please do not hesitate to contact us at foundation@vfw.org or 816-968-1128.

We know that every gift made to VFW Foundation is a choice. As the official 501(c)(3) of the VFW, we exist solely to support the programs and raise awareness necessary to operate the VFW. This is not possible without your generous support.

VFW FOUNDATION

406 W. 34th Street
Kansas City, MO 64111

Office 816.968.1128
Fax 816.968.2789

foundation@vfw.org
www.vfwfoundation.org