CAROLINAEAST FOUNDATION

PUBLIC NOTICE – VENDOR DATA INCIDENT

Blackbaud, Inc., one of our outside vendors, recently made us aware of a data security incident that may have involved personal data. Blackbaud is the global market leader in third party not-for-profit donor applications used by many charitable, health, and educational organizations in the U.S. and overseas.

What happened? On July 16, 2020, we were notified that Blackbaud had discovered and stopped a ransomware attack of Blackbaud's self-hosted platform in May 2020.

What information was involved?

Blackbaud specifically informed us that the cybercriminal did NOT access credit card information, bank account information, or social security numbers. According to Blackbaud, the cybercriminal did, however, remove a copy of a subset of Blackbaud customer data beginning as early as February 2020, which could have included information used for our fundraising purposes, such as names, addresses, email addresses, and donor profile information.

After investigation into this incident, we have determined that our Blackbaud Foundation databank(s) did NOT contain any financially sensitive information or any health information. As such, notice is not legally required, but rather, is posted here as a courtesy to our donors - so that they remain informed.

Blackbaud paid the cybercriminal's ransom demand with confirmation that the copy the cybercriminal removed had been destroyed.

Blackbaud does not believe this incident poses any risk to individuals, because, based on the nature of the incident, Blackbaud's research, and third party (including law enforcement) investigation, Blackbaud has 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. Blackbaud has reportedly hired a third-party team of experts to monitor the internet and dark web as an extra precautionary measure.

What are we doing? We investigated this incident and are reviewing relevant business practices regarding the security of Blackbaud data. Blackbaud reports that it has implemented numerous security changes. Blackbaud stated that it quickly identified the vulnerability associated with this incident and took swift action to fix it. Blackbaud has stated that it has confirmed through testing by multiple third parties that its fix withstands known attack tactics. Finally, Blackbaud is further hardening its environment through enhancements to access management, network segmentation, deployment of additional endpoint and network-based platforms.

What can you do? Based on the Blackbaud notice, this incident is not likely to result in a risk of harm to individuals, and as such, Blackbaud does not think there is anything more that needs to be done at this time relating to this specific incident.

NOTE: Notwithstanding this event, it is always a good idea for all individuals at all times to maintain the routine personal practice of remaining vigilant to cybercriminal scams (e.g., avoid clicking on email phishing scams such as malicious links or attachments and do not respond to illegitimate requests for personal information or money, etc.), which unfortunately are common occurrences. If suspicious activity is detected on any personal credit statements, credit reports or financial accounts, promptly report discrepancies to the applicable financial entity, law enforcement authorities, your State Attorney General's office, and/or the credit bureaus: Equifax (P.O. Box 74021, Atlanta, GA 30374; 800-685-1111; www.equifax.com), Experian (P.O. Box 2002, Allen, TX 75013; 888-397-3742; www.experian.com) or TransUnion (P.O. Box 1000, Chester, PA 19016; 800-916-8800; www.transunion.com). Additionally, for a free copy of their credit report and guidance on how to protect personal information with fraud alerts and security freezes, individuals may contact the credit bureaus and/or the Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, D.C. 20580, 1-877-IDTHEFT (438-4338), or www.ftc.gov/idtheft.

For more information about this incident, individuals can consult www.blackbaud.com/securityincident or call me directly (Telephone: 252-633-8247).

We sincerely apologize for any concern this may cause.

Thank you for the continued support of CarolinaEast Foundation.

Sincerely,

Jill Shumate Thompson
Executive Director
CarolinaEast Foundation

September 10, 2020