MUSC
Medical University
of South Carolina

September 11, 2020

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Dear <<b2b_text_1 (Title)>> <<last_name>>,

We are writing to inform you that one of our vendors, Blackbaud, Inc., recently made us aware of a data security incident that may have affected some of our patients' protected health information. As MUSC values you and takes the protection of your information very seriously, we want to share the details that we have received from Blackbaud surrounding this incident.

What happened?

On July 16, 2020, we were notified that Blackbaud, an outside vendor of MUSC, had discovered and stopped a ransomware attack on Blackbaud's self-hosted platform in May of 2020. Blackbaud is the global market leader in third-party, not-for-profit donor applications used by many charity, health, and educational organizations in the U.S. and abroad.

What information was involved?

Blackbaud has 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 in as early as February a copy of a subset of Blackbaud's customer data. The information removed included information used by MUSC for fundraising and donor relations purposes, such as individuals' names, contact information, demographic information, birth date, relationship and donation profile/history with MUSC, and some patient information (such as physician name, department visited and/or discharge date). 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 whose information was involved, 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 hired a third-party team of experts to monitor the dark web as an extra precautionary measure.

What are we doing?

MUSC is reviewing all relevant business practices and procedures regarding the security of your personal data. Blackbaud has reported that it has already implemented numerous security changes. Blackbaud has 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 Blackbaud's fix withstands all known attack tactics. Finally, Blackbaud has reported it is further hardening its environment through enhancements to access management and network segmentation, plus deployment of additional endpoint and network-based platforms.

What can you do?

Based on Blackbaud's notice, this incident is unlikely to result in a risk of harm to you, and as such, Blackbaud does not think there is anything more you need to do at this time relating to this specific incident.

As always, you should maintain your routine personal practices of remaining vigilant to cybercriminal scams, which are common occurrences. If you ever find suspicious activity on any of your personal credit statements/reports or financial accounts, you should promptly report discrepancies to law enforcement authorities, the applicable financial entity, and/or the credit bureaus: Equifax (PO Box 74021, Atlanta, GA 30374; 800-685-1111; www.equifax.com), Experian (PO Box 2002, Allen, TX 75013; 888-397-3742; www.experian.com) or TransUnion (PO Box 1000, Chester, PA 19016; 800-916-8800; www.transunion.com). Additionally, for a free copy of your credit report and guidance on how to protect your personal information with fraud alerts and security freezes, you 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.

On behalf of MUSC, we sincerely apologize and regret that this situation has occurred. For more information about this incident, kindly consult the Blackbaud website at blackbaud.com/securityincident. If you have additional questions about this incident, please do not hesitate to call our toll-free number at 1-877-461-2599 9:00 am – 6:30 pm EST Monday – Friday (excluding major holidays).

Kindest regards,

Kate Azizi

Kate Azizi
Vice President for Institutional Advancement, MUSC