1. What happened?

A third-party vendor named Blackbaud, which the Office of Institutional Advancement at Morehouse School of Medicine uses to maintain information about donors and potential donors, informed us of a criminal cyberattack that resulted in unauthorized access to certain information. Upon learning of this incident, we worked with our information technology and legal team to review Blackbaud's notification and determine what, if any, data may have been affected. Please know that we take this incident and the safeguarding of the security of our donors' personal information very seriously. It is important to note that Blackbaud's breach did not compromise credit card information, bank account information or Social Security numbers.

2. What is Blackbaud and why does the School use this vendor?

Blackbaud is the premier software and service provider for more than 25,000 nonprofit organizations, foundations and institutions of higher education worldwide. Morehouse School of Medicine has used this provider for many years to maintain information on donors and potential donors who may want to support our organization philanthropically. More specifically, the Office of Institutional Advancement uses Blackbaud's systems to manage and track alumni information, community relations, events and donor relations.

Current reports suggest that numerous Blackbaud customers in multiple countries were affected.

3. What exactly happened with Blackbaud's breach and did it affect my data?

Blackbaud informed us that they discovered and stopped a "ransomware" attack. During this time, hackers obtained a copy of certain information, such as contact information, demographic information, degree information and a history of donor's relationship with Morehouse School of Medicine. This data may or may not have contained your data. As mentioned above, credit card information, bank account information or Social Security numbers were not compromised. Blackbaud said they consulted with the FBI and cybersecurity experts and took steps to make sure the backup file was permanently destroyed.

4. When did the incident occur?

Blackbaud reports that it discovered and stopped the ransomware attack in May 2020. Morehouse School of Medicine was notified in July. Upon learning of the incident, the Office of Institutional Advancement began working in coordination with our IT, Legal and Marketing and Communications departments on a plan to investigate, learn the facts and communicate with constituents.

5. Should I be concerned that my personal data has been compromised?

According to the investigation by Blackbaud, as well as law enforcement and cybersecurity experts, we have no reason to believe that any data was or will be misused or will be disseminated or otherwise made available publicly. Out of an abundance of caution and to maintain transparency, we wanted to notify you of this incident.

6. What should I do?

At this time, there is no action required on your part. If we learn anything that suggests further steps should be taken, we will contact you immediately. As a best practice, we recommend that you remain vigilant and promptly report any suspicious activity to the proper law enforcement authorities.

7. Because of this breach, I'm concerned about the privacy of my information. What is Blackbaud doing to address the situation?

While we have confidence that the incident has been resolved by the vendor, we will continue to monitor the situation and take additional measures, if needed. Blackbaud has already implemented several changes to protect your data from any subsequent incidents. Its teams identified the vulnerability associated with this incident and took action to fix it. Blackbaud has tested its fix with multiple third parties, including the appropriate platform vendors, and assured Morehouse School of Medicine that the fix withstands all known cyber-attack tactics.

Our Commitment to You

While data breaches and ransomware attacks are becoming more common, this is not something that Morehouse School of Medicine ever wants to happen to our valued supporters. We take your privacy very seriously. We will continue to work with Blackbaud to monitor this situation. We sincerely apologize that this occurred through one of our third-party vendors and regret any inconvenience it may cause. If you have any questions or concerns regarding this matter, please contact us at giving@msm.edu.