Jackson College Foundation was recently made aware by our database vendor of a data security incident that **may** have involved information regarding our alumni and donors. Please know, that Jackson College Foundation does not store social security numbers, credit cards, or financial/banking information/data, and therefore, that information was not compromised.

What Happened and What Information Was Involved

Our database hosting vendor, Blackbaud—a leader in nonprofit finance, and fundraising software with more than 25,000 nonprofit customers around the world—recently experienced a ransomware attack and informed us that Jackson College Foundation was among the many affected parties. Blackbaud believes the attack took place in May 2020.

Blackbaud alerted us that a cybercriminal removed a copy of some of its customer files. It is believed that the files involved may have contained contact information, demographic data, and philanthropic support details.

According to Blackbaud, they paid a ransom for confirmation that the files were destroyed. Based on the nature of the incident, Blackbaud's research, and a 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.

They also report that their Cyber Security team, together with independent forensics experts and law enforcement, blocked the cybercriminal from accessing any additional files. Once the activities were contained and the breach secured, Blackbaud notified us of the incident. For additional information about this incident and Blackbaud's response, please visit Blackbaud's website.

What We Are Doing

Following notification, the College and Foundation activated our Information Security Incidence Response Plan protocols. This protocol, developed in partnership with Rehmann Group, was enacted and the situation was assessed, independently. 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, Blackbaud has implemented several changes to protect data from any subsequent incidents.

Blackbaud reports that its teams were able to identify the vulnerability associated with this incident, including the tactics used by the cybercriminal, and took action to fix it. It has confirmed through testing by multiple third parties that its fix withstands all known attack tactics. Additionally, they are accelerating their efforts to further harden their environment through enhancements to access management, network segmentation, deployment of additional endpoint, and network-based platforms.

What You Can Do

If you are a Jackson College Foundation donor, there is no action required by you at this time. As a best practice, we recommend you remain vigilant and promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities. Please note that no credit card or financial account information was compromised in this breach. Additional details are available on the Blackbaud website.

We share your frustration and concern and have expressed our extreme disappointment with Blackbaud. We're deeply sorry for this incident and regret any inconvenience this may cause. If you have further questions, please do not hesitate to contact us at foundation@jccmi.edu