ST MARY'S COLLEGE of MARYLAND
Foundation

18952 E. Fisher Road, St. Mary's City, MD 20686 | Tel: 240-895-4282 | Fax: 240-895-4454 | www.smcm.edu

Dear SMCM Community,

St. Mary's College of Maryland's Foundation takes the protection of our community members' information very seriously, which is why we are writing to let you know about a data security incident that may have involved your personal information.

To the extent that the data breach affects constituents residing in the UK or EU, please accept this letter as a notification pursuant to Article 33(2) of the General Data Protection Regulation ("GDPR"), although the data breach at issue is unlikely to result in a risk to the rights and freedoms of natural persons and notification may not be required.

We were recently notified that one of our third-party vendors, Blackbaud, was victim to a ransomware attack. Blackbaud (https://www.blackbaud.com) is a software vendor widely used by thousands of our colleagues in the education and fundraising sector and has over 30 years' experience.

What happened?

As recently explained to us, in May of 2020 Blackbaud discovered and stopped a ransomware attack. In a ransomware attack, cybercriminals attempt to disrupt the business by locking companies out of their own data and servers. After discovering the attack, Blackbaud's Cyber Security team—together with independent forensics experts and law enforcement—successfully prevented the cybercriminal from blocking their system access and fully encrypting files, ultimately expelling them from the system.

Blackbaud informed us that prior to locking the cybercriminal out, the cybercriminal removed a copy of our backup file containing personal information.

What information was involved?

The cybercriminal did not access credit card information, bank account information, or social security numbers. We do not store that information in this database with your protection in mind.

However, we have determined that the file removed may have contained your contact information, your constituent ID, and a history of your relationship with our organization, including donation dates and amounts, if applicable.

Because protecting their customers' data is their top priority, Blackbaud paid the cybercriminal's demand with confirmation that the copy they removed had been destroyed. Based on the nature of the incident, their 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.

How are we responding?

We are notifying you so that you can take immediate action to protect yourself. As is best practice, we recommend you remain vigilant and promptly report any suspicious activity or suspected identity theft to proper law enforcement authorities. In the unlikely event that such an investigation traces activity to our backup file, we ask that you let us know so that we can follow up.

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 informed us of corrective actions implemented and we will keep vigilant that Blackbaud is properly protecting data against future threats.

For more Information:

We sincerely apologize for this incident and regret any inconvenience it may cause you. Should you have any further questions or concerns regarding this matter, please do not hesitate to contact me at advancementoffice@smcm.edu.

Sincerely,

Jackie Wright

Jackie Wright
Director of Foundation Finance and Administration