

We are posting this notice to explain a data breach that may have involved your personal information. The breach occurred at our database service provider, Blackbaud Inc., one of the world's largest providers of financial and fundraising technology to nonprofits.

Importantly, we want to share with you that the data breach did not include credit card information, bank account information, or social security numbers.

Coastal Maine Botanical Gardens takes the protection and proper use of your information very seriously. We are therefore contacting you as a precautionary measure to explain the incident and provide you with steps you can take to protect your personal information.

The Nature of the Breach

On July 16, Blackbaud notified us of a data security breach affecting higher education institutions and nonprofits across the United States. Since that time, we have been working diligently to gather additional information. This data breach, which has recently been reported on widely by national media, occurred on February 7 and continued until May 20.

Blackbaud informed us that they discovered and stopped a ransomware attack and, with the help of independent forensics experts and law enforcement, successfully prevented the cybercriminal from blocking or encrypting files. Prior to locking the cybercriminal out, the cybercriminal removed a copy of our backup file containing your personal information. According to Blackbaud, they paid the cybercriminal a ransom to ensure the backup file was permanently destroyed.

The Information Involved

It is important to note that the cybercriminal did not access your credit card, bank account information, or social security number. Blackbaud has determined that the compromised file may have contained demographic data, including telephone numbers, email addresses, and mailing addresses, and information pertaining to your relationship with the Gardens, including philanthropic giving history.

Based on the nature of the incident, the research performed by Blackbaud, and third-party investigators, we have been told there is no reason to believe that any data went beyond the cybercriminal. Additionally, Blackbaud has indicated that they have no reason to believe any stolen data was or will be misused, or will be disseminated or otherwise made available publicly. Blackbaud has hired a third-party team of experts to continue monitoring for any such activity.

What Blackbaud Is Doing

Blackbaud's teams were able to quickly identify the vulnerability associated with this incident, including the tactics used by the cybercriminal, and took swift action to fix it. They have confirmed through testing by multiple third parties, including the appropriate platform vendors, that their fix withstands all known attack tactics. Additionally, Blackbaud is further enhancing its security controls, and, as part of their ongoing efforts to help prevent an incident like this in the future, they have already implemented several changes that will protect your data.

What You Can Do

While no credit card, bank account, or other sensitive information of that nature was compromised, as a best practice, we recommend you remain vigilant and promptly report any suspicious activity, phone calls, emails, or suspected identity theft to us and to the proper law enforcement authorities.

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 207-633-8027 or privacy@mainegardens.org.