Blackbaud Incident Frequently Asked Questions

1. What happened?
Blackbaud, a vendor utilized by Margaret Mary Health Foundation was the victim of a cyber-attack. On July 16, 2020, Blackbaud informed us they experienced a ransomware attack in May of 2020. In a typical ransomware attack, a criminal actor accesses data and encrypts it so the rightful owner of the data can no longer access it until a ransom payment is made. In this case, the attacker did not block access to data, but was able to remove a copy of certain data files from the Blackbaud system and demanded a ransom payment in return for assurances the files would be destroyed. Blackbaud paid a ransom to the attacker and received the attacker's assurance the stolen data was destroyed.

2. When did it happen?
Blackbaud became aware of the ransomware attack in May of 2020. The vendor informed us of the incident on July 16, 2020.

3. What information was involved?
The information that was potentially compromised was contained in back-up files for certain Blackbaud products. The information included name, address, telephone number, email address, gender, date of birth, marital status, spouse name, medical record number, donation history, limited notes and publicly available financial data. Blackbaud has stated the attackers could not access usernames, passwords, credit card information, bank account information or Social Security numbers because of security controls they use to protect this sensitive data. In fact, Margaret Mary Health Foundation does not have Social Security numbers in our system.

4. Was my medical information involved?
This incident did not involve your Margaret Mary Health medical records. In fact, Margaret Mary Health Foundation does not have any health/medical information from your electronic medical record in our system.

5. Who is Blackbaud?
Blackbaud provides our philanthropy functions with a data platform for fundraising, donor communications and information management. Blackbaud provides these services to more than 35,000 organizations world-wide. They are an industry leader for services of this nature.

6. Why was I notified?
You received a letter from us because you are in our system as either a donor, event attendee, organization, team member or patient of Margaret Mary Health. Margaret Mary Health Foundation chose to notify you because it takes seriously the confidentiality and security of constituent and donor information and wants to ensure everyone is well-informed and able to take appropriate precautions against any potential compromise of their information.

7. Why am I just learning about this?
We did not learn of this incident until July 16, 2020 and issued communications to our constituents as soon as we felt we had sufficient, meaningful information to share. We are concerned Blackbaud did not notify us of this incident until two months after they learned of it and are addressing those concerns with them.

8. Is my information at risk?
Blackbaud has communicated it does not believe any data was or will be made available publicly, primarily based on the assurance they received from the attacker that the data has been destroyed. If we become of aware of further material information, we will notify those involved as appropriate and advise of any additional steps they should take to protect themselves.

9. Were Margaret Mary Health's computer systems involved in this incident?
No. This attack occurred solely on Blackbaud's computer system and did not involve our own computer systems or network in any way.

10. Who is the attacker?
At this time, the identity of the attacker is not known. Unfortunately, this is typical with this type of cyber-attack.

11. What has Margaret Mary Health done in response to this incident?
Margaret Mary Health took immediate steps to investigate this incident, with a focus on determining exactly what occurred, what information may have been exposed and what additional protections Blackbaud is putting in place. As part of the investigation, Margaret Mary Health is seeking additional information about the incident from Blackbaud and other sources. We also are proactively communicating with all of those potentially affected so they can take any additional steps they deem necessary to protect themselves.

12. What are you doing to protect constituent information in the future?
We are assessing the efficacy of Blackbaud's security controls and will continue to advocate on our constituents' behalf that Blackbaud take every precaution to prevent and protect against any misuse of their information.

13. Is there anything I should be doing to protect myself?
We are recommending our constituents remain vigilant toward any solicitations for charitable contributions they may receive and to report any suspicious activity or identity theft to law enforcement authorities.

14. Is credit monitoring being offered to constituents?
According to information provided by Blackbaud, cybercriminals didn't access any credit card or bank account information because of security controls they use on this sensitive data. In fact, we do not have Social Security numbers or health/medical information from your electronic medical record in our system. Accordingly, free credit card monitoring is not being offered at this time.

15. I have other questions. How can I get more information?
We are here to help. Please call us at 866.601.3555 and we will answer your questions to the best of our ability.