Frequently Asked Questions

Q. What happened?
A. In May, Blackbaud (a third-party service provider) 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; and ultimately expelled them from our system. Prior to our locking the cybercriminal out, the cybercriminal removed a copy of a subset of data from their self-hosted (private cloud) environment. This is the place where Blackbaud stores the information contained in our solutions. Because protecting customers' data is their top priority, Blackbaud paid the cybercriminal's ransomware demand with confirmation that the copy they removed had been destroyed. Based on the nature of the incident, Blackbaud's research, and third party (including law enforcement) investigation, we have 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. Blackbaud notified us of this incident in July.

Q. Who is Blackbaud, and what is their relationship with to Catholic Social Services?
A. Blackbaud is a third-party service provider that provides cloud software, services, expertise, and data intelligence to a variety of organizations. This includes nonprofits, foundations, corporations, education institutions, and healthcare institutions. We use Blackbaud for our database.

Q. How did you determine to notify me?
A. We worked in coordination with our legal counsel to review the information that was potentially accessed by the cybercriminal and to determine our notification obligations with applicable laws. We postal mailed letters to people whose mailing address we had and who made any donation between January 2020 and May 2020. For donations made through a phone or email only portal, we have posted a notification on our web-site.

Q. Why didn't you notify me sooner?
A. We notified you as soon as we could after our own due diligence.

Q. Do you think my information will be released?

A. We have received assurances from Blackbaud that, based on their investigation, research and third-party investigation, they have 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. As a precautionary measure, Blackbaud has hired a team of experts to monitor the dark web for any information linked to this incident, and they have found no evidence that any information was ever released. The dark web monitoring will continue indefinitely.

Q. What information typically triggers a need for identify protection?
A. There are various laws throughout the world that determine whether an organization has to provide identity protection. In most cases, the need to supply identity protection exists when Social Security numbers (or a country's equivalent) are accessed. NOTE: Catholic Social Services donor database, Blackbaud Raisers Edge, does not capture or store social security numbers or bank account information.

Q. What can someone do with my bank account information?
A. The Federal Reserve has noted that payments fraud involving use of ACH information remains rare due largely to the technological innovations banks and payments providers have put in place to identify and mitigate fraud at the point where funds are dispersed and deposited. In many cases, access to an account

number will only allow the person who has the account's number to transfer money ***to that account***. It is true there are cases when it becomes possible to set up a direct debit to a vendor, however most banks require verification signatures to set up a direct debit. Additionally, banks have protection systems designed to monitor suspicious activities on their customers' accounts.

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. Also, Blackbaud paid the cybercriminal's ransom demand with confirmation they deleted the information. They also engaged a third party which is conducting ongoing monitoring of the dark web and we have found no evidence of information being made available publicly. In the unlikely event that were to happen, Blackbaud will notify Catholic Social Services. If you have additional concerns, some general best practice actions you can take include the following:

1. Examine daily bank account activity and reconcile bank accounts regularly
2. Utilize your bank's debit block features to ensure unauthorized debits cannot be made on your bank accounts so you can pre-authorize any account debits
3. Confirm any requests via email to change a vendor's bank account with an actual call back to the vendor