Blackbaud Security Incident Web Notification

Maintaining the security of our foundation and donor information is of the utmost importance to Ascension Providence Rochester Foundation. We recently received notice from Blackbaud – a third party that provides many non-profit organizations, including many health care and higher-education institutions, across the world with fundraising and engagement software – that the company experienced a ransomware attack in May 2020 that involved the perpetrators accessing certain foundation information. Blackbaud has assured Ascension Providence Rochester Foundation that the perpetrators did not access sensitive information, such as bank or full credit card information, or social security numbers, and that Blackbaud believes the perpetrators have destroyed the information they copied.

Blackbaud paid the ransom demanded by the cybercriminals in exchange for confirmation of the destruction of the copy. Blackbaud reported it has no reason to believe the data went beyond the original perpetrators. Blackbaud hired a third-party team of forensic experts to assist them with their investigation and, out of an abundance of caution, will continue monitoring for any disclosure of the copied information. We will continue to work with Blackbaud to ensure our comfort with their cybersecurity remedial measures with respect to this matter.

You can read Blackbaud's statement about the incident here:
https://www.blackbaud.com/securityincident.

When did it happen?
Blackbaud first discovered the incident on May 14, 2020. It stopped the cyberattack on May 20, 2020, and worked to understand what information was exposed and who was affected. Blackbaud notified us on July 16, 2020. Since then, Ascension Providence Rochester Foundation has been diligently working to gather information about who may have been directly impacted by the incident.

What information was involved?
Depending on the system affected and the information provided by and retained on each individual, the information that was included in the back-up data copy may be different. Most information affected was demographic data, such as name and address. It could have included some or all of the following information: name, address, email, date of birth, phone number, fax number, spouse's name, and other publicly available information about you. Certain databases that were affected may have also included high level notes about your donation history, including amount and dates of donation, payment related information, such as check date and number (but not account number). Full credit card, social security, and any other banking information was not included. There may also have been some limited care related information affected for some individuals.

How do I know if I was affected?
Ascension Providence Rochester Foundation is reaching out via mail or email when possible to potentially affected individuals. We may not have up-to-date contact information for all individuals affected and may not be able to reach them directly. If you have concerns that you were affected but did not receive a notice, contact 248-652-5346.

How should I protect myself?
While most of the information included in the ransomware attack is also publicly available, it is important you remain vigilant in responding to anyone trying to contact you to obtain information about you. In this case, we recommend that you also use caution in responding to donation solicitations. Blackbaud is

continuing to monitor the situation for any further disclosure of the affected information. If we learn there is evidence of any further wrongdoing with the affected data, we will alert you.

What steps have been taken to address the incident?
Blackbaud hired a third-party team of forensic experts to assist them with their investigation and, out of an abundance of caution, will continue to monitor for any disclosure of the affected information.

Ascension Providence Rochester Foundation is currently working with Blackbaud to ensure our comfort with their cybersecurity remedial measures. We take the protection of our information very seriously and will continue to work with Blackbaud to ensure it is secure.

We are committed to providing clear, transparent communication about the incident as well as receiving feedback and answering questions. We continue to monitor Blackbaud's response, including the steps that Blackbaud is taking to protect our information moving forward.