Blackbaud Notification to JPS Foundation

The information below relates to a data security incident involving Blackbaud, Inc., a service provider of the JPS Foundation, the philanthropic arm of JPS Health Network. Our organization takes our data protection responsibilities very seriously. JPS has launched its own investigation and further details are below, including steps taken in response.

The Incident

On July 16, 2020, the JPS Health Network Finance Department was contacted by Blackbaud, one of the world's largest providers of customer relationship management systems for not-for-profit organizations. A message from company representatives said Blackbaud had been the victim of a "data security incident that started on Feb. 7, 2020, and possibly continued intermittently until May 20, 2020." The cybercriminal was unsuccessful in blocking access to the database involved in the attack. However, the cybercriminal was able to remove a copy of a subset of several of their clients' data. This included a subset of JPS Foundation data used for donor prospect research.

What information was involved?

JPS Foundation wants to reassure its donors that a detailed forensic investigation was undertaken, on behalf of Blackbaud, by law enforcement and third-party cyber security experts.

Blackbaud has confirmed that the investigation found no encrypted information, such as Social Security numbers and bank account information or passwords, was accessible. Blackbaud also confirmed that no credit or debit card information was part of the data theft. **JPS Foundation does not collect Social Security numbers, bank account information or credit and debit card information.**

JPS Foundation data accessed by the hackers in the Blackbaud database *may* have contained some of the following information:

- Names and titles
- Addresses and contact details such as phone numbers and e-mail addresses
- Philanthropic interests, giving capacity and summary giving history to JPS

What actions were taken by Blackbaud?

Blackbaud has informed JPS that in order to protect donors' data and mitigate potential identity theft, the company met the cybercriminal's ransomware demand. Blackbaud reports it has received assurances from the hackers and third-party experts that the data was destroyed.

Blackbaud continues to monitor the web in an effort to verify the data accessed by the hackers has not been misused.

JPS response

JPS Health Network's IT division immediately launched its own investigation and continues to work with Blackbaud to understand why there was a delay between finding the breach and notifying us, as well as what actions Blackbaud is taking to increase its security.

We do not believe there is a need for our donors to take any action at this time. As a best practice, we recommend people remain vigilant and promptly report any suspicious activity or suspected identity theft to the proper authorities.

For questions related to the security incident, please contact the JPS Foundation. The foundation also may be reached at jpsfoundation@jpshealth.org.

Please be assured we take data protection very seriously and are grateful for our community's continued support of JPS Health Network. While JPS was not the target of this attack, nor was it the only organization affected, we are taking time to learn from this third-party incident and to review our own security practices and system configurations to better protect your information.