Blackbaud Data Security Incident

The following information relates to a data security incident involving Blackbaud, Inc., one of Ball State University Foundation's third-party service providers. Please know that Ball State Foundation takes data protection responsibilities very seriously. We have launched our own investigation and further details are below, including steps we have taken in response and what you can do to protect yourself.

The Incident

On July 16, 2020, we were contacted by Blackbaud, one of the world's largest providers of customer relationship management systems for not-for-profit organizations and the higher education sector. Company representatives informed us that a Blackbaud service provider had been the victim of a ransomware attack that culminated in May 2020. The cybercriminal was unsuccessful in gaining access to the database involved in the attack. However, the cybercriminal was able to remove a copy of a subset of several of their client's data. This included a subset of Ball State Foundation data.

What information was involved?

We would like to reassure you 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 that **no encrypted information, such as Social Security numbers and bank account information or passwords, was obtained by the cybercriminals**. Blackbaud also confirmed that **no credit or debit card information was part of the data theft**. Furthermore, as best practice Ball State Foundation does not store credit card information or Social Security numbers in its system.

The Ball State Foundation data accessed by the cybercriminal in the Blackbaud database *may* have contained some of the following information:

- Public information such as name, title, date of birth, spouse
- Addresses and contact details such as phone numbers and e-mail addresses
- Philanthropic interests, giving capacity and summary giving history to Ball State Foundation
- Educational attainment

What actions were taken by Blackbaud?

We have been informed by Blackbaud that in order to protect all data and mitigate potential identity theft, it met the cybercriminal's ransomware demand. Blackbaud has advised us that it has received assurances from the cybercriminal and third-party experts that the data was

destroyed. Blackbaud has been monitoring the web in an effort to verify the data accessed by the cybercriminal has not been misused.

Steps we have taken in response

We immediately launched our own investigation and have taken the following steps:

- We are notifying affected donors, friends, and alumni to make them aware of this breach of Blackbaud's systems so they can remain vigilant;
- We are working with Blackbaud to understand why there was a delay between it finding the breach and notifying us, as well as what actions Blackbaud is taking to increase its security;
- We are taking steps to learn how many other parties in the higher education and the wider not-for-profit sector have been affected.

Additionally, we are exploring all options to ensure this does not happen again, including revisiting our relationship with Blackbaud.

What you can do
As a best practice, we recommend you remain vigilant and promptly report any suspicious activity or suspected identity theft to the proper authorities.

For questions related to the security incident, contact Ball State Foundation staff member Stephen Wachtmann, associate vice president of finance and treasurer, at sjwachtmann@bsu.edu or 765-285-7072 (direct) or 888-I-GO-4-BSU (toll-free).

We will continue to work with Blackbaud to investigate this incident. We very much regret the inconvenience that this data breach may have caused. One of Ball State Foundation's core values is ensuring the privacy rights of alumni and friends, and we promise to do everything in our power to live up to the trust you have placed in the Ball State Foundation.

Thank you for your partnership and support.