DEFUR VORAN
Attorneys, Business Counselors & Neighbors

Nicholas M. Tokar
ntokar@defur.com
Reply to Muncie office

September 18, 2020

The Honorable Mr. Bob Ferguson
Washington State Office of the Attorney General
1125 Washington St NE
PO Box 40100
Olympia, WA 98504

RE: Ball State University Foundation

Dear Mr. Attorney General:

We are writing to notify you of a data security breach suffered by our client, the Ball State University Foundation ("BSUF"). After analysis, we now believe that 755 residents of your state may have had personal information, consisting of names and SSN/TINs, illegally accessed by cybercriminals, who breached the systems of Blackbaud, Inc., a third-party service provider. Notice of the breach, as required by law, is being sent to the aforementioned 18 residents of your state.

In summary, on or about July 16, 2020, BSUF was 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 BSUF 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 BSUF data.

Blackbaud informed BSUF that a detailed forensic investigation was undertaken, on behalf of Blackbaud, by law enforcement, and third-party cyber security experts. BSUF has 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.

BSUF immediately launched its own investigation and have taken the following steps:

- Notifying affected donors, vendors, friends, and alumni to make them aware of this breach of Blackbaud's systems so they can remain vigilant;
- 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;
- Taking steps to learn how many other parties in the higher education and the wider not-for-profit sector have been affected.

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

If you have any further questions, please contact me.

Sincerely,

Nicholas M. Tokar

BALL STATE UNIVERSITY
Foundation

September 10, 2020

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.

What happened?

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.

However, our independent analysis has concluded that the cybercriminals may have accessed files which contained your Social Security Number/Tax ID Number.

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.

What We are Doing?

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.

We encourage you to remain vigilant for incidents of fraud and identity theft by regularly reviewing your account statements and monitoring your credit reports for suspicious activity. You also might consider placing a fraud alert or security freeze on your credit bureau reports. Everyone is allowed one free credit report per year from each of the three major credit bureaus. To learn how to obtain your free annual credit report under federal law, visit AnnualCreditReport.com or call (877) 322-8228.

A victim of fraud is eligible to receive one free credit report from each of the major credit bureaus:

TransUnion LLC: (800)916-8800; TransUnion.com; P.O. Box 2000, Chester, PA 19016

Experian: (866)200-6020; Experian.com; P.O. Box 2002, Allen TX 75013

Equifax: (888)766-0008; Equifax.com; P.O. Box 740241, Atlanta, GA 30374

In addition, you can contact the Federal Trade Commission to learn more about how to protect yourself from becoming a victim of identity theft and how to repair identity theft:

Federal Trade Commission Consumer Response Center
600 Pennsylvania Avenue,
NW Washington, DC 20580
1-877-IDTHEFT (438-4338)
ftc.gov/idtheft

For More Information

For questions related to the security incident, contact Ball State University Foundation at foundation@bsu.edu or 765-285-8312 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.