

CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

CAROLYN PURWIN RYAN
cpurwin@c-wlaw.com

Admitted in PA and NJ

JASON MICHAEL GOODWIN
jgoodwin@c-wlaw.com

450 Sentry Parkway, Suite 200
Blue Bell, Pennsylvania 19422

Telephone: (610) 567-0700
Fax: (610) 567-0712

www.C-WLAW.com

A Mid-Atlantic Litigation Firm

Visit us online at
www.C-WLAW.com

August 21, 2020

Via Email (securitybreach@atg.wa.gov)

Office of the Attorney General
1125 Washington Street SE
PO Box 40100
Olympia, WA 98504-0100

RE: Blackbaud Security Incident Notification

To Whom It May Concern:

I serve as counsel for the West Virginia University Foundation (“WVUF”), and provide this notification to you of a recent data security incident suffered by Blackbaud, Inc. (“Blackbaud”), a provider of cloud-based data management services. On July 16, 2020, WVUF was notified by Blackbaud that it had discovered and stopped a ransomware attack that occurred in May 2020. Blackbaud’s systems that were affected by the attack included a database containing certain information about WVUF’s donors. According to the notification provided by Blackbaud, the attacker(s) may have acquired an unknown amount of data maintained within Blackbaud’s database. Blackbaud informed us that it paid a ransom to the attacker and obtained confirmation that the compromised information had been destroyed and is no longer in the possession of the attacker(s). According to Blackbaud, and as far as we know, there is no indication that any of the compromised information has been subject to misuse or to further disclosure. Notably, Blackbaud has assured the WVUF that no credit card information, bank account information, username and passwords, or Social Security numbers were impacted as a result of this incident. As Blackbaud provided only general information regarding the scope of the incident, WVUF immediately began an internal investigation. As a result of the internal investigation, WVUF has discovered that date of birth information was present within the database and not encrypted by Blackbaud as it relates to 1,015 Washington residents.

WVUF immediately provided general notification regarding the incident to the WVUF community on July 24, 2020. While we believe the information potentially impacted, including the circumstances of the incident, provide little to no risk of harm to the affected individuals, the WVUF is providing supplemental notification to the affected individuals on August 21, 2020 to ensure compliance with Washington State law. A copy of the drafted letter is attached. WVUF is taking steps to comply with all applicable notification obligations.

Please contact me should you have any questions.

Very truly yours,

CIPRIANI & WERNER, P.C.

By:



Carolyn Purwin Ryan

To our Alumni and Friends,

On July 24th, the WVU Foundation provided notification¹ of a security incident experienced by our service provider, Blackbaud. We are providing this additional notification in order to provide additional information that has become available since our initial email. According to Blackbaud, they were the victim of a ransomware incursion beginning on February 7, 2020, which continued until May 20, 2020. Blackbaud is one of the world's largest providers of customer relationship management systems for not-for-profit organizations and the higher education sector. While Blackbaud prevented the cybercriminal from encrypting Blackbaud data, the cybercriminal was able to remove a copy of a subset of constituent data from several of Blackbaud's clients, including the WVU Foundation.

As mentioned in our initial email, Blackbaud confirmed that their investigation found that **no encrypted information, such as Social Security numbers, bank account, and credit and debit card information, was accessible.** Data accessed by the cybercriminal *may* have contained public constituent information such as name, title, date of birth, spouse, phone numbers and e-mail addresses. Additionally, the impacted data may have contained information regarding your giving history. No further information has been identified as being impacted.

Blackbaud also confirmed that they paid the cybercriminal's demand and received confirmation that the removed data was destroyed. Blackbaud has engaged third-party experts to monitor the dark web in an effort to verify the data accessed by the cybercriminal has not been misused or released and intends to continue such monitoring on an indefinite, 24/7/365 basis. Blackbaud has assured us that they have taken steps to secure their environment to prevent future incidents from occurring.

We do not believe there is a need for you to take any action at this time. As a best practice, we recommend that you remain vigilant and promptly report any suspicious activity or suspected identity theft to the proper authorities, as well as the major credit reporting agencies whose information is provided below.

¹ You may not have received the WVU Foundation's initial communication regarding this incident if we do not have a valid email address on file.

TransUnion

Fraud Victim Assistance Dept.
P.O. Box 6790
Fullerton, CA 92834
1-800-680-8289
www.transunion.com

Experian

National Consumer Assistance
P.O. Box 1017
Allen, TX 75013
1-888-397-3742
www.experian.com

Equifax

Consumer Fraud Division
P.O. Box 105069
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

For more information on this incident, visit the Foundation's [web site](#). If you have questions, contact Mike Phillips, WVU Foundation Senior Director of Information Systems and Security, mphillips@wvuf.org or 304-284-4054.

We will continue to work with Blackbaud to investigate this incident. We deeply regret any inconvenience this data breach of Blackbaud's system may have caused. Please be assured we take data protection very seriously and are grateful for the continued support of our alumni and friends.

Sincerely yours,

Cindi Roth
President and CEO
WVU Foundation