GRESHAM | SAVAGE
ATTORNEYS AT LAW

Matt.Wilcox@GreshamSavage.com · San Diego Office
(619) 794-0050 · *fax* (619) 615-2180

August 27, 2020

VIA EMAIL AND U.S. MAIL

Office of the North Dakota Attorney General
Consumer Protection and Antitrust Division
1050 E. Interstate Avenue, Suite 200
Bismarck, ND 58503-5574
ndag@nd.gov

RE: Notice of a Data Breach

Ladies and Gentlemen:

We are writing to you on behalf of California Baptist University, a nonprofit private university located in Riverside, California ("**CBU**"), to inform you of a data security breach at Blackbaud (one of CBU's outside vendors), that involved the personal information of 16 residents of North Dakota.

Blackbaud provides database management platforms and processes charitable donations for 40,000 nonprofit clients across the United States, including CBU. Blackbaud informed CBU on July 16, 2020, that an intrusion into their system occurred earlier this year (at some point between February 7, 2020, and May 20, 2020), but that Blackbaud, in consultation with independent forensics experts and law enforcement, had prevented the attackers from encrypting all of Blackbaud's records and had expelled them from Blackbaud's system. Blackbaud has informed CBU that it paid a ransom for the destruction by the attackers of their copy of the information accessed, so as to avoid dissemination of that information by the attackers, and that, based upon the nature of the incident, Blackbaud's own research, and law enforcement investigation, Blackbaud does not believe the information accessed will be misused or made public.

Blackbaud has confirmed that that the hackers did not access credit card information or have access to unencrypted bank account information, social security numbers, user names, or passwords--all sensitive financial information was encrypted, and CBU itself does not store any social security numbers, credit card or bank information, driver's license numbers, or similar highly confidential information on Blackbaud's servers. The hackers, however, may have accessed:

- Personal details (name, gender, date (and, in some cases, place) of birth, marital status, alumni status/other connection with CBU, which could include GPA, area of study, graduation date);

- Contact details (email, street address, and telephone numbers); and

- Records of giving to CBU, some (very few) birthplaces, and some educational information (GPA, area of study, graduation date, etc.).

Blackbaud has informed CBU that, in response to the breach, they have implemented several changes to protect data from any further breaches: they have identified--and fixed--the vulnerability that was exploited by the attackers, and have confirmed through testing by multiple third parties, that their fix withstands all currently known attack routes; and they are working to further enhance the security of customers' data.

Because the data accessed by the hackers included donors' unencrypted names and dates of birth, CBU, by letter dated August 25, 2020, has notified each of the sixteen (16) affected North Dakota residents of the data breach by first class U.S. mail. Attached please find a copy of the notification letter sent to these residents.

If you have any questions or require additional information, please contact me at Matt.Wilcox@greshamsavage.com, or by phone at (619) 344-2980.

Very truly yours,

Matt Wilcox, of
GRESHAM SAVAGE
NOLAN & TILDEN,
A Professional Corporation

JMW:pgp
Enclosure

Letter to ND Residents

CBU California Baptist University

951.689.5771
951.343.4578 (fax)
calbaptist.edu

8432 Magnolia Avenue, Riverside, CA 92504

August 25, 2020

[Donor Name]
[Address]
[City, State Zip]

RE: NOTICE OF A DATA BREACH

Dear [Donor],

We are writing to inform you about a data security breach at Blackbaud, Inc. one of CBU's outside vendors, that involved some of your personal information. No unencrypted sensitive identifying information was accessed, and there is no immediate action you need take in response to the breach. Nevertheless, we take the protection and proper use of your information seriously, and so are notifying you of the incident, out of an abundance of caution, to let you take such precautions as you deem advisable.

What Happened

By now, you may have read about a ransomware attack on Blackbaud, which provides database management platforms and processes charitable donations for 40,000 nonprofit clients across the United States, including CBU. Blackbaud has informed CBU that the intrusion occurred at some point between February 7, 2020, and May 20, 2020; but that Blackbaud, in consultation with independent forensics experts and law enforcement, successfully prevented the attackers from encrypting all of Blackbaud's records and expelled them from Blackbaud's system. Blackbaud has informed us that it paid a ransom for the destruction by the attackers of their copy of the information accessed, so as to avoid dissemination of that information by the attackers. Based upon the nature of the incident, Blackbaud's own research, and law enforcement investigation, Blackbaud does not believe the information accessed will be misused or made public. As an extra precaution, they have also retained a team of experts to monitor the dark web.

Blackbaud has posted its own account of the incident, which can be accessed at https://www.blackbaud.com/securityincident?utm_source=U.

How This Affects You

CBU uses Blackbaud's Raiser's Edge database and related products, and has for several years. Last month Blackbaud notified CBU that CBU's backup file maintained by Blackbaud had been accessed during the intrusion.

What Information Was Involved

The information CBU stores on the Raiser's Edge database is generally publicly available information (e.g. names, addresses, phone numbers, email addresses, etc.); **CBU does not itself store any social security numbers, credit card or bank information, driver's license numbers, or similar highly confidential information on Blackbaud's servers**. We have also verified with Blackbaud that the hackers did not access credit card information or have access to unencrypted bank account information, social security numbers, usernames, or passwords--all sensitive financial information was encrypted.

The hackers, however, may have accessed the following information:

- Personal details (name, gender, date (and, in some cases, place) of birth, marital status, alumni status/other connection with CBU, which could include GPA, area of study, graduation date, and records of giving to CBU, if any)
- Contact details (email, street address, and telephone numbers)

Our Response

We sincerely regret any inconvenience this data security incident may have caused you. We have been informed by Blackbaud that they have already implemented several changes to protect your data from any further breaches: they have identified - and fixed - the vulnerability that was exploited by the attackers, and have confirmed through testing by multiple third parties, that their fix withstands all currently known attack routes; and they are working to further enhance the security of your data.

What You Can Do

We recommend that you remain vigilant, and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities. To file a complaint with the FTC, please visit www.ftc.gov/idtheft or call (877) ID - THEFT (438-4338). We also attached additional information regarding how to obtain a free credit report and options you can take to guard against identity theft.

More Information

Should you have any questions or concerns regarding this matter, please do not hesitate to contact me at (951) 343-4492.

Sincerely,

Paul J. Eldridge, J.D.
Vice-President
University Advancement

California Baptist University
8432 Magnolia Avenue
Riverside, CA 92504

YOU HAVE RECEIVED A DATA BREACH NOTICE-

ADDITIONAL INFORMATION REGARDING STEPS YOU CAN TAKE

As a precautionary matter, we recommend that you remain vigilant and closely monitor your financial account statements and credit reports. Suspicious account activity should be reported to the financial institution or company with which the account is maintained. Any fraudulent activity or suspected identity theft should be promptly reported to law enforcement.

You may obtain a free copy of your credit report from each of the three major credit reporting agencies on an annual basis (once every 12 months) by visiting https://www.annualcreditreport.com and completing and submitting a free credit report request form. Alternatively, you may purchase a copy of your credit report by contacting any one of the three national credit reporting agencies whose contact information for credit report assistance is provided below:

Equifax
Automated Service Telephone Number: (800) 685-1111
Customer Service Telephone Number: (866) 349-5191
Equifax Information Services LLC P.O. Box 740241
Atlanta, GA 30374-0241
https://www.equifax.com

Experian
Telephone Number to Order Credit Report: (888) 397-3742
Credit Report by mail is unavailable.
535 Anton Blvd., Suite 100
Costa Mesa, CA 92626
https://www.experian.com

TransUnion
Telephone Number to Order Credit Report: (800) 888-4213
TransUnion LLC P.O. Box 1000
Chester, PA 19016
https://www.transunion.com

You may also consider having each of those three major credit reporting agencies place a fraud alert on your credit report. An initial fraud alert will stay on your credit file for at least 90 days. The alert will inform any creditor that submits an inquiry about your credit of possible fraudulent activity and request that the inquiring creditor contact you before establishing any account in your name. You can place a fraud alert by visiting the websites of the credit reporting agencies listed above.

Additional information about steps you can take to help protect against harm from a data breach, including identity theft, is available online on the Federal Trade Commission ("FTC") website: https://www.identitytheft.gov. You can also contact the FTC at (877)-ID-Theft (438-4338) or at: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.