BakerHostetler

Baker&Hostetler LLP

Key Tower
127 Public Square, Suite 2000
Cleveland, OH 44114-1214

T 216.621.0200
F 216.696.0740
www.bakerlaw.com

David E. Kitchen
direct dial: 216.861.7060
dkitchen@bakerlaw.com

DECEMBER 15, 2020

VIA EMAIL (NDAG@ND.GOV)

Office of the Attorney General
State Capitol
600 E. Boulevard Avenue
Bismarck, North Dakota 58505

Re: Incident Notification

Dear Sir or Madam:

We are writing on behalf of our client, American Indian College Fund, to notify you of a security incident involving North Dakota residents. American Indian College Fund is an organization that provides assistance to American Indians seeking college degrees.

On July 16, 2020, American Indian College Fund was notified by Blackbaud of a ransomware attack on Blackbaud's network that the company discovered in May of 2020. Blackbaud is a cloud-based software company that provides services to thousands of schools, hospitals, and other non-profits. Blackbaud reported that it conducted an investigation, determined that backup files containing information from some of its clients had been taken from its network, and an attempt was made to encrypt files to convince Blackbaud to pay a ransom. Blackbaud paid a ransom and obtained confirmation that the stolen files had been destroyed. Blackbaud also reported that it has been working with law enforcement.

Upon learning of the incident from Blackbaud, American Indian College Fund conducted its own investigation of the Blackbaud services used by American Indian College Fund and the information provided by Blackbaud to determine what information was involved in the incident. On November 18, 2020 American Indian College Fund determined that the backup files contained certain information pertaining to 2,51 North Dakota residents, including the residents' names and full dates of birth.

Beginning today, December 15, 2020, American Indian College Fund is providing written notice to the North Dakota residents by mailing letters via United States Postal Service First-Class

mail. A sample copy of the notification letter is enclosed. American Indian College Fund has also established a dedicated phone number where the individuals may obtain more information regarding the incident.

Blackbaud has informed American Indian College Fund that they identified and fixed the vulnerability associated with this incident, implemented several changes that will better protect data, and are undertaking additional efforts to improve the security of its environment through enhancements to access management, network segmentation, and deployment of additional endpoint and network-based platforms. American Indian College is no longer utilizing Blackbaud for its donor and alumni engagement and its data has been removed from Blackbaud's cloud-based system.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

David E. Kitchen
Partner

Enclosure

AMERICAN INDIAN COLLEGE FUND

EDUCATION IS THE ANSWER

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

We are writing to notify you that we, along with many other institutions, were notified by Blackbaud that it experienced a security incident. This notice explains the incident and the measures taken in response.

What Happened?

Blackbaud is a cloud-based software company that provides services to thousands of schools, hospitals, and other non-profits. On July 16, 2020, Blackbaud notified us that it had discovered a ransomware attack on Blackbaud's network occurring in May 2020. Blackbaud reported that it conducted an investigation, and it was determined that backup files containing information from its clients had been taken from its network. An attempt was made to encrypt files to convince Blackbaud to pay a ransom. Blackbaud paid a ransom and obtained confirmation that the files that had been removed had been destroyed. Blackbaud reported that it has been working with law enforcement.

Upon learning of the incident from Blackbaud, we conducted our own investigation of the Blackbaud services we use, and the information provided by Blackbaud to determine what information was involved in the incident. On November 18, 2020 we determined that the backup files contained certain information pertaining to you.

What Information Was Involved?

The backup file involved contained your name and full date of birth. Blackbaud assured us that no encrypted data such as Social Security numbers, bank account information, addresses, and credit/debit card information was accessible to the unauthorized person. Blackbaud also assured us that the backup file has been destroyed by the unauthorized individual and there is no reason to believe any data was or will be misused or will be disseminated or otherwise made available publicly.

What We Are Doing.

We are notifying you of this incident and sharing the steps that we, and Blackbaud, are taking in response. Blackbaud has informed us that they identified and fixed the vulnerability associated with this incident, implemented several changes that will better protect your data and are undertaking additional efforts to improve the security of its environment through enhancements to access management, network segmentation, and deployment of additional endpoint and network-based monitoring tools. The College Fund is no longer utilizing Blackbaud for our donor and alumni engagement and our data has been removed from their cloud-based system.

For More Information.

We regret that this occurred and apologize for any inconvenience. Should you have any further questions or concerns regarding this matter, please do not hesitate to contact us at [redacted] between 8:00 am and 5:30 pm Central Time, Monday through Friday, excluding major U.S. holidays.

Sincerely,

Cheryl Crazy Bull

Cheryl Crazy Bull
President/CEO