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

September 14, 2020

VIA E-MAIL (NDAG@ND.GOV)

Office of the Attorney General
State Capitol
600 E. Boulevard Avenue
Department 125
Bismarck, ND 58505

Re: Incident Notification

Dear Sir or Madam:

We are writing on behalf of our client, Mercy Corps ("MC"), to notify you of a data security incident involving 697 North Dakota residents.

On July 16, 2020, MC 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 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 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, MC conducted its own investigation of the Blackbaud services it uses and the information provided by Blackbaud to determine what information was involved in the incident. On August 5, 2020, MC determined that the backup file contained the name and date of birth of 697 North Dakota residents.

Beginning today, MC is providing written notice via United States Postal Service First-Class mail to the North Dakota residents in the same form as the enclosed letter. MC has provided a phone number and email address where all individuals may obtain more information regarding the incident.

Blackbaud has informed MC that they identified and fixed the vulnerability associated with this incident, implemented several changes that will better protect data from any subsequent incidents, and are undertaking additional efforts to harden their environment through enhancements to access management, network segmentation, and deployment of additional endpoint and network-based platforms.

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

Sincerely,

David E. Kitchen
Partner

Enclosure

MERCY CORPS

<<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 and many other institutions were recently notified by Blackbaud that it experienced a security incident. This notice explains the incident and measures taken in response.

What Happened

Blackbaud is a cloud-based software company that provides services to thousands of schools, hospitals, and other nonprofits. On July 16, 2020, Blackbaud notified us that it had discovered a ransomware attack on Blackbaud's network in May 2020. Blackbaud reported that it conducted an investigation, determined that backup files containing information from 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 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 August 5, 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, and credit and 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 from any subsequent incidents, and are undertaking additional efforts to harden their environment through enhancements to access management, network segmentation, and deployment of additional endpoint and network-based platforms.

For More Information

Mercy Corps takes your data security and privacy very seriously. We remain in contact with Blackbaud regarding the details of this incident, and we are continuing to monitor their response. 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 donorservices@mercycorps.org or (503)896-5001.

Sincerely,

Beth deHamel
Interim CEO