September 14, 2020

Kevin M. Scott
Direct: 312/602-5074
Fax: 312/698-7474
kevin.scott@bclplaw.com

BRYAN CAVE LEIGHTON PAISNER LLP
161 North Clark Street Suite 4300
Chicago IL 60601 3315
T: +1 312 602 5000
F: +1 312 602 5050
www.bclplaw.com

Attorney General Gordon MacDonald

Office of the Attorney General
33 Capitol Street
Concord, NH 03302
attorneygeneral@doj.nh.gov

Dear Attorney General MacDonald,

We represent Bluegrass Care Navigators ("BCN"), a private hospice, located in Lexington, Kentucky, with respect to a data security incident described in more detail below. BCN takes the security and privacy of the information in its control very seriously, and is taking steps to prevent a similar incident from occurring in the future.

On July 16, 2020, we were notified by Blackbaud of a data security incident. The incident involved a ransomware attack, which was successfully defeated. However, the attacker removed the backup data files of hundreds of organizations worldwide, including BCN. With the assistance of law enforcement and forensic investigators, Blackbaud was able to receive confirmation that the backup data was destroyed and has confirmed that it has not been found anywhere on the internet at this time.

We have received assurances that the data has not gone beyond the attacker, was not or will not be misused, disseminated or otherwise made publicly available. The information within the data files may have contained patient contact information, demographic information, and limited health information (e.g. the dates the patient was visited by our volunteers). The attacker did not access credit card information, bank account information, or Social Security number.

One (1) New Hampshire resident's personal information was contained within the data file. A notification letter to the estate of this individual was mailed by first class mail on September 14, 2020. A sample copy of the notification letter is included with this letter.

Blackbaud has already implemented several changes that will protect the data from any subsequent incidents. First, Blackbaud's teams were able to quickly identify the vulnerability associated with this incident, including the tactics used by the attacker, and took swift action to fix it. Blackbaud has confirmed through testing by multiple third parties, including the appropriate platform vendors, that its fix withstands all known attack tactics. Additionally, they are accelerating their efforts to further harden their environment through enhancements to access management, network segmentation, deployment of additional endpoint and network-based platforms.

BCN remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me.

Very truly yours,

Kevin M. Scott

KMS:llh
Attachment

BLUEGRASS care navigators

Expert. Connected. Care.

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

To the Guardian or Executor for
<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

To the Guardian or Executor for <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

We are contacting you to make you aware of an issue recently brought to our attention by our third-party software vendor, Blackbaud. Blackbaud is one of the world's largest providers of customer relationship management systems for not-for-profit organizations. We take the security of your loved one's personal information very seriously, and we sincerely apologize for any concern this incident may cause.

On July 16, 2020, we were notified by Blackbaud of a data security incident. The incident involved a ransomware attack, which was successfully defeated. However, the attacker removed the backup data files of hundreds of organizations worldwide, including Bluegrass Care Navigators. With the assistance of law enforcement and forensic investigators, Blackbaud was able to receive confirmation that the backup data was destroyed and has confirmed that it has not been found anywhere on the internet at this time.

We have received assurances that the data has not gone beyond the attacker, was not or will not be misused, disseminated or otherwise made publicly available. It is important to note that your loved one's information was contained in those data files, and *may* have contained their contact information, demographic information, and limited health information (e.g. the dates they were visited by our volunteers). **The attacker did not access their credit card information, bank account information, or Social Security number.**

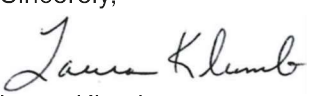
Please know that we take this incident and the security of your loved one's personal information very seriously. Ensuring the safety of our constituents' data is of the utmost importance to us. In order to prevent a reoccurrence, Blackbaud has already implemented several changes that will protect their data from any subsequent incidents.

First, Blackbaud's teams were able to quickly identify the vulnerability associated with this incident, including the tactics used by the attacker, and took swift action to fix it. Blackbaud has confirmed through testing by multiple third parties, including the appropriate platform vendors, that its fix withstands all known attack tactics. Additionally, they are accelerating their efforts to further harden their environment through enhancements to access management, network segmentation, deployment of additional endpoint and network-based platforms.

We recommend that you review the additional information enclosed, which contains important steps you can take to further protect your loved one's personal information.

We very much regret any inconvenience this incident may cause you. Should you have any further questions or concerns regarding this matter, please call 1-???-???-????, Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Time.

Sincerely,



Laura Klumb
Vice President, Philanthropy

Additional Important Information

For residents of *Hawaii, Illinois, Iowa, Maryland, Michigan, Missouri, North Carolina, Virginia,* and *Vermont*: It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing payment card account statements and monitoring your credit reports for unauthorized activity. You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

***For residents of Iowa*:** You are advised to report any suspected identity theft to law enforcement or to the Attorney General.
For residents of *Oregon*: You are advised to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.
For residents of New Mexico: You are advised to review personal account statements and credit reports, as applicable, to detect errors resulting from the security incident, and that you have rights pursuant to the federal Fair Credit Reporting Act. Please see the contact information for the Federal Trade Commission listed below.

For residents of Illinois, Maryland, New York, North Carolina, and Rhode Island:
You can obtain information from the Maryland, New York, North Carolina, and Rhode Island Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023

New York Office of the Attorney General
Consumer Frauds & Protection Bureau
120 Broadway - 3rd Floor
New York, NY 10271
breach.security@ag.ny.gov

North Carolina Office of the Attorney General
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-566-7226
www.ncdoj.com

Rhode Island Office of the Attorney General
Consumer Protection
150 South Main Street
Providence RI 02903
1-401-274-4400
www.riag.ri.gov

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Ave, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.identitytheft.gov

For residents of Massachusetts and Rhode Island: You have the right to obtain a police report if you are a victim of identity theft.

For residents of all states:
Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf), Experian (https://www.experian.com/fraud/center.html), or Transunion (https://www.transunion.com/fraud-victim-resource/place-fraud-alert). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. Initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; (5) Proof of current address, such as current utility or telephone bill, bank or insurance statement; (6) legible photocopy of government-issued identification card (state driver's license or ID card, military identification, etc.); and (7) if you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. It is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348-5788
www.equifax.com/personal/credit-report-services/
800-525-6285

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013-9544
www.experian.com/freeze/center.html
888-397-3742

TransUnion (FVAD)
P.O. Box 160
Woodlyn, PA 19094
www.transunion.com/credit-freeze
888-909-8872

More information can also be obtained by contacting the Federal Trade Commission listed above.