September 4, 2020

Office of the Attorney General
1125 Washington St. SE
Olympia, WA 98504
SecurityBreach@atg.wa.gov

Re: Legal Notice of Information Security Breach Pursuant to Wash. Rev. Code § 19.255.010

To Whom It May Concern:

In accordance with the above-referenced provision of Washington law, I write to inform you of an information security incident affecting residents of Washington.

We are one of the many nonprofit clients affected by the recent data security incident at Blackbaud Inc., a data service vendor for the Hydrocephalus Association (HA). On July 16, 2020, Blackbaud sent an email to HA stating that it had discovered a security incident in May of 2020. Blackbaud determined that an unauthorized third party had removed a copy of certain non-financial data, including data from HA and other Blackbaud clients, at some point between February 7, 2020 and May 20, 2020. Although Blackbaud told us that it believes the data was destroyed after Blackbaud made a payment in response to a demand from the unauthorized third party, we cannot independently confirm the destruction of the data. Blackbaud has provided additional details about this incident on its website.

As a result of our investigation, we determined on August 14, 2020 that specific information our members shared with us through membership communications, registrations, or surveys may have been part of this breach. Our investigation to date has identified that the information may have included name, address, a member's connection to HA, the date of birth of a member or their loved one with hydrocephalus, and limited health information (e.g., patient's name, age of diagnosis, type of hydrocephalus, and/or comorbidities or complications). Bank account or credit card information was not impacted by this incident, as HA does not retain financial information within our database.

Upon learning of this incident, we took immediate steps to investigate the incident and to identify and notify individuals affected. We are not aware of any misuse to date of the compromised information, and Blackbaud has communicated its confidence that the data was destroyed. Regardless, we are reviewing our work with Blackbaud to ensure it meets Blackbaud's contractual commitments and are in the process of evaluating our relationship with Blackbaud more generally.

We plan to notify 835 potentially affected individuals who are residents of Washington. Enclosed is a copy of the notification that will be sent to affected individuals via email on or about September 4, 2020.

The notification to individuals includes (1) a description of the incident and the type of personal information at issue; (2) the actions taken by HA to protect personal information from further unauthorized access; (3) HA's address and email address to contact for further information and assistance; (4) information about how to place a fraud alert or security freeze on a credit report; (5) the toll-free numbers and addresses for the major consumer reporting agencies; (6) the phone number, address, and website for the Federal Trade Commission, and a statement that individuals can obtain information on

identity theft from this source; and (7) advice that directs the individual to remain vigilant by reviewing account statements and monitoring free credit reports.

If you have any questions or need further information regarding this incident, please contact me at diana@hydroassoc.org or (240) 483-4472.

Sincerely,

Diana Gray, President and CEO
diana@hydroassoc.org
240.483.4472

Enclosure

September 4, 2020

Dear xxxxxxxx

We are writing to let you know of a recent data security incident at Blackbaud Inc., a data service vendor for the Hydrocephalus Association (HA). Blackbaud is a leading provider of software services and hosts files or backups for hundreds of schools, foundations, and nonprofits like HA around the world. Blackbaud recently informed us that it discovered and resolved a cybersecurity incident impacting its systems, which affected many of its nonprofit clients, including HA.

What Happened?

We are contacting you regarding this incident with Blackbaud because some of your personal information may have been disclosed. On July 16, 2020, Blackbaud sent an email to HA stating that it had discovered a security incident in May of 2020. Blackbaud determined that an unauthorized third party had removed a copy of certain non-financial data, including data from HA and other Blackbaud clients, at some point between February 7, 2020 and May 20, 2020. Although Blackbaud told us that it believes the data was destroyed after Blackbaud made a payment in response to a demand from the unauthorized third party, we cannot independently confirm the destruction of the data. Blackbaud has provided additional details about this incident on its website.

What Information Was Involved?

First and foremost, please be reassured that your bank account or credit card information was not involved in this incident, as HA does not retain financial information within our database.

On August 14, 2020, we determined that specific information you shared with us through membership communications, registrations, or surveys may have been part of this breach. This could include name, address, your connection to HA, the date of birth of you or your loved one with hydrocephalus, and limited health information (e.g., patient's name, age of diagnosis, type of hydrocephalus, and/or comorbidities or complications), to the extent you provided this information.

For clarity, please know that the incident did not involve information associated with our patient registry, "HAPPIER." Information for that patient registry is stored in a separate database at the University of Utah, outside of Blackbaud. That information is de-identified, meaning the information that could link it to you has been removed, and it is not part of this incident. Information stored in HydroAssist, our mobile app, is also not a part of this incident. HydroAssist data is stored in a separate database outside of Blackbaud.

What We Are Doing.

We are extremely frustrated about this event and take this matter very seriously. Safeguarding your personal information is a top priority for us. We are not aware of any misuse to date of the compromised information, and as previously stated, Blackbaud has communicated its confidence that the data was destroyed. Regardless, upon learning of this incident, we immediately began working to investigate the incident and to identify and notify individuals affected.

We require Blackbaud to keep our information confidential and to maintain security procedures to minimize the risk of information security incidents. If an information security incident does occur, Blackbaud is required to notify us, to work with us to mitigate negative consequences from the incident, and to implement procedures to prevent a similar incident from occurring again. We will review our work with Blackbaud to ensure it meets that commitment and are in the process of evaluating our relationship with Blackbaud more generally.

What You Can Do.

Although no credit card or bank account information was compromised as part of this incident, given the increased threats to privacy in our world we recommend that you remain vigilant and regularly review and monitor all of your credit history to guard against any unauthorized transactions or activity. We also recommend that you closely monitor your account statements and notify your financial institution if you suspect any unauthorized activity. Additionally, you should not provide personal information in response to electronic communications regarding security breaches. Attachment A contains more information about steps you can take to protect yourself against fraud and identity theft.

For More Information

Please be assured that we are taking steps to address the incident and to protect the security of your data. If you have any questions about this notice or the incident, please feel free to contact us at security@hydroassoc.org.

ATTACHMENT A

Additional Information

To protect against possible fraud, identity theft or other financial loss, we encourage you to remain vigilant, to review your account statements and to monitor your credit reports. Provided below are the names and contact information for the three major U.S. credit bureaus and additional information about steps you can take to obtain a free credit report, and place a fraud alert or security freeze on your credit report. If you believe you are a victim of fraud or identity theft you should consider contacting your local law enforcement agency, your State's attorney general, or the Federal Trade Commission.

INFORMATION ON OBTAINING A FREE CREDIT REPORT

U.S. residents are entitled under U.S. law to one free credit report annually from each of the three major credit bureaus. To order your free credit reports, visit www.annualcreditreport.com or call toll-free (877) 322-8228.

INFORMATION ON IMPLEMENTING A FRAUD ALERT, CREDIT FREEZE, OR CREDIT LOCK

To place a fraud alert, credit freeze, or credit lock on your credit report, you must contact the three credit reporting agencies below:

Equifax:
Equifax Information Services LLC
P.O. Box 105788
Atlanta, GA 30348
1-888-298-0045
www.equifax.com

Experian:
Credit Fraud Center
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion:
Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19022-2000
1-800-680-7289
www.transunion.com

Fraud Alert: Consider contacting the three major credit reporting agencies at the addresses below to place a fraud alert on your credit report. A fraud alert indicates to anyone requesting your credit file that you suspect you are a possible victim of fraud. A fraud alert does not affect your ability to get a loan or credit. Instead, it alerts a business that your personal information might have been compromised and requires that business to verify your identity before issuing you credit. Although this may cause some short delay if you are the one applying for the credit, it might protect against someone else obtaining credit in your name.

To place a fraud alert, contact any of the three major credit reporting agencies listed above and request that a fraud alert be put on your file. The agency that you contacted must notify the other two agencies. A fraud alert is free and lasts 90 days, but can be renewed.

Credit Freeze: A credit freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report until the freeze is lifted. When a credit freeze is in place, no one—including you—can open a new account. As a result, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing, or other services.

Placing a credit freeze is free. To place a credit freeze, contact all three credit reporting agencies listed above and provide the personal information required by each agency to place a freeze, which may include:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.); and
7. If you are a victim of identity theft, a copy of either a police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

When you place a credit freeze, you will be provided a PIN to lift temporarily or remove the credit freeze. A credit freeze generally lasts until you lift or remove it, although in some jurisdictions it will expire after seven years.

Credit Lock: Like a credit freeze, a credit lock restricts access to your credit report and prevents anyone from opening an account until unlocked. Unlike credit freezes, your credit can typically be unlocked online without delay. To lock your credit, contact all three credit reporting agencies listed above and complete a credit lock agreement. The cost of a credit lock varies by agency, which typically charges monthly fees.

You may also contact the U.S. Federal Trade Commission ("FTC") for further information on fraud alerts, credit freezes, credit locks, and how to protect yourself from identity theft. The FTC can be contacted at 400 7th St. SW, Washington, DC 20024; telephone 1-877-382-4357; or www.consumer.gov/idtheft.

ADDITIONAL RESOURCES

Your state Attorney General may also have advice on preventing identity theft, and you should report instances of known or suspected identity theft to law enforcement, your State Attorney General, or the FTC.

District of Columbia Residents: The Attorney General can be contacted at the Office of the Attorney General, 441 4th Street NW, Washington, DC 20001; (202) 727-3400; or https://oag.dc.gov/.

Maryland Residents: The Attorney General can be contacted at Office of Attorney General, 200 St. Paul Place, Baltimore, MD 21202; (888) 743-0023; or http://www.oag.state.md.us.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain any police report filed in connection to the incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

North Carolina Residents: The Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; (919) 716-6400; or http://www.ncdoj.gov.

New Mexico Residents: You have rights under the federal Fair Credit Reporting Act (FCRA), which governs the collection and use of information pertaining to you by consumer reporting agencies. For more information about your rights under the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

Rhode Island Residents: The Attorney General can be contacted at (401) 274-4400 or http://www.riag.ri.gov/. You may also file a police report by contacting local or state law enforcement agencies.