LEWIS BRISBOIS BISGAARD & SMITH LLP

David E. Artman
888 SW Fifth Avenue, Suite 900
Portland, Oregon 97204-2025
David.Artman@lewisbrisbois.com
Direct: 971.712.2805

September 4, 2020

VIA E-MAIL

Attorney General Bob Ferguson
Office of the Attorney General
1125 Washington Street SE
PO Box 40100
Olympia, WA 98504-0100
E-Mail: SecurityBreach@atg.wa.gov

Re: Notification of Data Security Incident

Dear Attorney General Ferguson:

We represent Children's Cancer Association ("CCA"), a nonprofit organization headquartered in Portland, Oregon. The purpose of this letter is to notify you that CCA was recently informed that one of its vendors, Blackbaud, Inc. ("Blackbaud"), experienced a data security incident that may have involved personal information related to CCA donors and beneficiaries. CCA takes the protection of all information within its control very seriously and is working with Blackbaud to prevent a similar incident from occurring in the future.

1. **Nature of the Security Incident.**

On July 16, 2020, Blackbaud reported that it had experienced a data security incident that may have involved unauthorized access to CCA data. Upon learning this information, CCA immediately launched an investigation, which included requesting information from Blackbaud about the incident, data involved, and its forensics investigation. According to Blackbaud, the unauthorized access may have occurred between February 7, 2020 and May 20, 2020. On August 7, 2020, CCA learned that dates of birth and/or certain medical information for a limited number of people could have been accessed without authorization.

2. **Number of Washington Residents Affected.**

CCA notified 1,752 residents of Washington via written letter beginning on September 4, 2020. A sample copy of the notification letter sent to the affected individuals is included with this correspondence.

3. Steps Taken Relating to the Incident.

Upon learning of the incident, CCA immediately launched an independent investigation and worked with Blackbaud to ensure that its data was secure. Blackbaud confirmed that the matter had been reported to law enforcement and that the Federal Bureau of Investigation (FBI) was actively involved in the investigation. Blackbaud further reported that it has no reason to believe that any data was or will be misused. Blackbaud further advised that it had not detected any information relating to the incident through its continuous dark web monitoring activities.

Furthermore, CCA has notified the potentially-affected individuals and offered them 12 months of complimentary identity monitoring services through ID Experts.

4. Contact Information.

CCA remains dedicated to protecting the personal information in its control. Please do not hesitate to contact me should you have any questions.

Sincerely,

David E. Artman of
LEWIS BRISBOIS BISGAARD & SMITH LLP

DEA

Enclosure: Sample Consumer Notification Letter

Children's Cancer Association
JoyRx.org

C/O ID Experts
P.O. Box 1907
Suwanee, GA 30024

To Enroll, Please Call:
(833) 755-1022
Or Visit:
https://app.myidcare.com/account-creation/protect
Enrollment Code: **[CODE]**

[Insert Name]
[Insert Address]

Semptember 4, 2020

Re: Notice of Data Security Incident

Dear [Name],

I am writing to provide additional information about the data security incident that a third-party vendor we use for fundraising, Blackbaud, Inc. ("Blackbaud"), experienced, and about which we emailed all donors and beneficiaries on July 24, 2020. Our investigation recently determined that a limited amount of your information could have been involved in the incident. I therefore wanted to provide you with steps that can be taken to help protect your information and offer you complimentary identity monitoring services as detailed below. As a reminder, Blackbaud does not store credit card, Social Security numbers or bank account information for CCA donors or beneficiaries, so this information was not involved in the incident.

What Happened? As stated in our July 24th email, on July 16, 2020, Children's Cancer Association ("CCA") learned that Blackbaud had experienced a data security incident that may have involved CCA data. According to Blackbaud, unauthorized individuals may have accessed information in certain Blackbaud databases between February 7, 2020 and May 20, 2020. Upon learning this information, we immediately launched an investigation. Blackbaud has confirmed that much of the information in the affected databases was protected by encryption, and therefore inaccessible to the unauthorized individuals. However, on August 7, 2020, we learned that a limited amount of your personal information was not encrypted, and therefore could have been accessed without authorization as a result of the incident. Blackbaud has informed us that they have no reason to believe that any data has or will be misused, or that any data will be shared publicly.

What Information Was Involved? The information involved may have included your name and [insert variable text].

What Are We Doing? As soon as we discovered the incident, we launched an investigation and worked with Blackbaud to ensure that our data is now secure. We also received confirmation that Blackbaud had reported this incident to the Federal Bureau of Investigation. We will provide law enforcement with all cooperation needed to hold the perpetrators accountable. We've also confirmed that Blackbaud will continuously monitor the Internet for any exposure of personal information. We are now providing you with information to help protect your personal information, including offering you complimentary identity monitoring services for 12 months.

What You Can Do: Although Blackbaud has informed us that it has no evidence suggesting that your information has been, or will be, misused, we encourage you to review the recommendations on the following page and take any necessary precautions to further protect your personal information. We also encourage you to take advantage of the complimentary identity monitoring services that we are offering for 12 months through ID Experts. The services include 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, ID Experts will help you resolve issues if your identity is compromised. You can enroll in the services by calling (833) 755-1022 or going to https://app.myidcare.com/account-creation/protect and using the Enrollment Code

provided above. MyIDCare experts are available Monday through Friday from 6 am - 6 pm Pacific Time. Please note the deadline to enroll is December 8, 2020.

For More Information: If you have any questions about this letter, please call (833)-755-1022. We regret any worry or inconvenience that this may cause you.

Sincerely,

Danielle York
President/General Manager
Children's Cancer Association

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

TransUnion	**Experian**	**Equifax**	**Free Annual Report**
P.O. Box 1000	P.O. Box 9532	P.O. Box 740241	P.O. Box 105281
Chester, PA 19016	Allen, TX 75013	Atlanta, GA 30374	Atlanta, GA 30348
1-800-916-8800	1-888-397-3742	1-800-685-1111	1-877-322-8228
www.transunion.com	www.experian.com	www.equifax.com	annualcreditreport.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Security Freeze: You have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. There is no charge to place, lift or remove the security freeze. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission	**Maryland Attorney General**	**North Carolina Attorney General**	**Rhode Island Attorney General**
600 Pennsylvania Ave, NW	200 St. Paul Place	9001 Mail Service Center	150 South Main Street
Washington, DC 20580	Baltimore, MD 21202	Raleigh, NC 27699	Providence, RI 02903
consumer.ftc.gov, and	oag.state.md.us	ncdoj.gov	http://www.riag.ri.gov
www.ftc.gov/idtheft	1-888-743-0023	1-877-566-7226	401-274-4400
1-877-438-4338			

You also have certain rights under the Fair Credit Reporting Act (FCRA), including: to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information, as well as others. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

Personal Information of a Minor: You can request that each of the three national credit reporting agencies perform a manual search for a minor's Social Security number to determine if there is an associated credit report. Copies of identifying information for the minor and parent/guardian may be required, including birth or adoption certificate, Social Security card, and government issued identification card. If a credit report exists, you should request a copy of the report

and immediately report any fraudulent accounts to the credit reporting agency. You can also report any misuse of minor's information to the FTC at https://www.identitytheft.gov/. For more information about Child Identity Theft and instructions for requesting a manual Social Security number search, visit the FTC website: https://www.consumer.ftc.gov/articles/0040-child-identity-theft.