September 9th, 2020

To whom it may concern,

Blackbaud, a vendor our organization uses as our database and point of sale system, alerted us on July 16th 2020 that they had experienced a data breach. In our database 57,024 individuals met the criteria for being notified based on the data we retain (Name, address, birth date).

Communication steps with KidsQuest Children's Museum patrons:

1. We emailed all patrons in our database that we had email addresses for and had not opted out of email communication. This email went out on July 21st, 2020 to 19,465 email addresses and was resent to all email addresses that had not opened the original email on July 25th, 2020.
2. A post card was mailed to patrons in our database that met the requirements for contacting (Name, address, and birthdate) that were not included in the email list. These post cards were sent to 19,465 addresses.

Attached you will find:

- The email that was sent to us notifying us of the breach of our customers information at Blackbaud
- A copy of the email we sent to all patrons within our database with an email address on file and had not opted out of our email communication (regardless of the amount of information we had stored) – delivered to 19,465 email inboxes
- A copy of the mailer we sent to those affected without an email on file or have opted out of email communications – mailed to 16,384 addresses

Please do not hesitate to reach out if more information is needed.

Thank you.

Stephanie Philio
Technology Support Specialist
KidsQuest Children's Museum
www.kidsquestmuseum.org
425-637-8100

blackbaud

Dear Stephanie,

Please see a personalized note below for your organization from our Chief Information Officer. Thank you.

Dear Stephanie,

We are writing to notify you about a particular security incident that recently occurred. Please review this email for a personalized link, next steps and resources created for your organization specifically.

What Happened

The Cybercrime industry represents an over trillion-dollar industry that is ever-changing and growing all the time—a threat to all companies around the world. At Blackbaud, our Cyber Security team successfully defends against millions of attacks each month and is constantly studying the landscape to ensure we are able to stay ahead of this sophisticated criminal industry. **In May of 2020, we discovered and stopped a ransomware attack. In a ransomware attack, cybercriminals attempt to disrupt the business by locking companies out of their own data and servers. After discovering the attempted attack, our Cyber Security team—together with independent forensics experts and law enforcement—successfully prevented the cybercriminal from blocking our system access and fully encrypting files; and ultimately expelled them from our system.**

Prior to our locking the cybercriminal out, the cybercriminal removed a copy of a subset of data from our self-hosted environment. The cybercriminal did not access credit card information, bank account information, or social security numbers. Because protecting our customers' data was our top priority, we paid the cybercriminal's demand with confirmation that the copy they removed had been destroyed.

Based on the nature of the incident, our research, and third party (including law enforcement) investigation, we have no reason to believe that any data went beyond the cybercriminal, was or will be misused; or will be disseminated or otherwise made available publicly. In accordance with regulatory requirements and in an abundance of caution, we are notifying all organizations whose data was part of this incident and are providing resources and tools to help them assess this incident.

What This Means for Your Organization Specifically

Our public cloud environment (Microsoft Azure and Amazon Web Services) and most of our self-hosted datacenters, products and customers were not part of this incident, but we have confirmed the following specific to your organization:

- A copy of your Blackbaud Altru backup was part of this incident. Again, the file the cybercriminal removed a copy of did not contain any credit card information. Further, the cybercriminal did not gain access to bank account information, usernames, passwords, or social security numbers stored in your database because they were encrypted. None of your data was lost or corrupted as a result of this incident.

And again, based on the nature of the incident, our research, and third party (including law enforcement) investigation, we have no reason to believe that any data went beyond the cybercriminal, was or will be misused; or will be disseminated or otherwise made available publicly. We have hired a third-party team of experts to monitor the dark web as an extra precautionary measure.

We have created a resource page for you at www.blackbaud.com/incidentresources that features a toolkit with a step-by-step guide to help you as you digest this information. It also contains answers to key questions, links to educational webinars (hosted by Rich Friedberg, Blackbaud's Chief Information Security Officer and Cameron Stoll, our Head of Privacy), information about our future plans, and other resources.

It is unlikely but possible, depending on jurisdiction, that our customers may have to make further notifications to constituents or other third parties. Your toolkit provides a written guide to notification laws and access to a webinar that helps you assess potential notification requirements in your jurisdictions. We advise you to also consult with your organization's legal counsel to understand any notification requirements. We want to continue to be your partner through this incident. If you determine that you do need to notify your constituents, we have included templates in your toolkit to make it easier.

To ensure all your questions are answered as quickly as possible, we encourage you to first review the resources we provided at the link above. If you still have questions after reviewing these resources, we are here to help. Please contact the dedicated team we have established for this incident:

- **North and South America:** 1-855-907-2099 between 9 a.m. and 9 p.m. ET Monday – Friday

We understand this situation is frustrating. This was a very sophisticated attack, and while we were able to defend against it for the most part, we realize this is still requiring that you invest time to review the situation, and that you may need to invest time to take follow-up actions. We apologize for this and will continue to do our very best to supply help and support as we and our customers jointly navigate any necessary response to the cybercriminal's actions.

Sincerely,

Todd Lant
Chief Information Officer

KidsQuest Children's Museum

July 21, 2020

Dear KidsQuest Family,

We were recently made aware of a security incident at Blackbaud, our vendor for our point of sales system and database. Blackbaud is one of the largest companies in its industry and serves non-profits around the globe. They informed us that at some point between February and May of this year, they experienced a ransomware attack described as a large operation that involved the data from multiple nonprofit organizations.

KidsQuest Children's Museum holds the privacy and security of donor information as a top priority and we are taking this incident very seriously. Blackbaud has stated that the cybercriminals did not obtain donor credit card information, because it is encrypted. KidsQuest Children's Museum does not collect or keep social security numbers or bank account information.

Blackbaud has stated that they believe the data affected in the ransomware attack has been destroyed and they have hired an external security team to monitor for evidence to the contrary. Data accessed in the attack may have included names, birth dates, and contact information, including telephone numbers, email addresses and mailing addresses, according to Blackbaud. The data may also have included purchase and donation history.

Individuals(s) that could have been effected:

We encourage you check and report any oddities on your credit report to one of these agencies:

Experian 1-888-397-3742
Equifax 1-800-685-1111
TransUnion 1-888-909-8872
Innovis 1-800-540-2505

Blackbaud has stated that they have no reason to believe there will be any public disclosure of data. With the safety of your information as our highest priority, KidsQuest Children's Museum leadership has taken a very active role in working with Blackbaud to determine how this security breach occurred, and how to prevent it from happening again. Blackbaud's **official statement** describes the incident in greater detail.

If you have any questions or would like further information, please email us **here** or visit our **website** for more details.

Sincerely,

Elaine Morse
Chief Financial Officer
KidsQuest Children's Museum

KidsQuest
Children's Museum
1116 108th Ave NE • Bellevue, WA 98004

August 2020

Dear KidsQuest patron,

We were made aware of a security incident at Blackbaud, our vendor for our point of sales system. They informed us that at some point between February and May of this year, they experienced a ransomware attack described as a large operation that involved the data from multiple nonprofit organizations.

KidsQuest Children's Museum holds the privacy and security of donor information as a top priority and we are taking this incident very seriously. Blackbaud states that the cybercriminals did not obtain donor credit card information, because it is encrypted. KidsQuest Children's Museum does not collect or keep social security numbers or bank account information.

Blackbaud states they believe the data affected in the ransomware attack has been destroyed and they have hired an external security team to monitor for evidence to the contrary. Data accessed in the attack may have included names, birth dates, and contact information, including telephone numbers, email addresses and mailing addresses, according to Blackbaud. The data may also have included purchase and donation history.

We encourage you check and report any oddities on your credit report to one of these agencies:

Experian 1-888-397-3742, **Equifax** 1-800-685-1111, **TransUnion** 1-888-909-8872 **Innovis** 1-800-540-2505

If you have any questions or would like further information, please email us at *blackbaudsecuritybreach@kidsquestmuseum.org* or visit www.kidsquestmuseum.org for FAQs

Sincerely,

Elaine Morse
Chief Financial Officer
KidsQuest Children's Museum
(425) 637-8100 – *please leave a detailed message*