



THE PLACE WHERE AWESOME LIVES

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

August 17, 2020

F7193-L01-0000001 P001 T00001 *****MIXED AADC 159
SAMPLE A SAMPLE - L01_KCMGC_NON-CANADA
APT 123
123 ANY ST
ANYTOWN, US 12345-6789



Extra1

Dear Sample A Sample:

Kohl Children’s Museum of Greater Chicago (“Kohl Children’s Museum”) writes to inform you of a recent incident that may affect the privacy of some of your information. On Thursday, July 16, 2020, Kohl Children’s Museum received notification from one of its third-party vendors, Blackbaud, Inc. (“Blackbaud”), of a cyber incident. Blackbaud is a cloud computing provider that offers customer relationship management and financial services tools to organizations, including Kohl Children’s Museum. Upon receiving notice of the cyber incident, we immediately commenced an investigation to better understand the nature and scope of the incident and any impact on Kohl Children’s Museum data. This notice provides information about the Blackbaud incident, our response, and resources available to you to help protect your information from possible misuse, should you feel it necessary to do so.

What Happened? Blackbaud reported that, in May 2020, it experienced a ransomware incident that resulted in encryption of certain Blackbaud systems. Blackbaud reported the incident to law enforcement and worked with forensic investigators to investigate. Following its investigation, Blackbaud notified its customers that an unknown actor may have accessed or acquired certain Blackbaud customer data. Blackbaud reported that data was exfiltrated by the unknown actor at some point before Blackbaud locked the unknown actor out of the environment on May 20, 2020. Upon learning of the Blackbaud incident, Kohl Children’s Museum immediately began to determine what, if any, sensitive Kohl Children’s Museum data was potentially involved. This investigation included working diligently to gather further information from Blackbaud to understand the scope of the incident. On or about August 5, 2020, Kohl Children’s Museum received further information from Blackbaud that allowed us to confirm the information potentially affected may have contained personal information.

What Information Was Involved? Our investigation determined that the involved Blackbaud systems contained your name and Extra2. Please note that, to date, we have not received any information from Blackbaud that your information was specifically accessed or acquired by the unknown actor.

What We Are Doing. The confidentiality, privacy, and security of information in our care are among our highest priorities, and we take this incident very seriously. As part of our ongoing commitment to the security of information in our care, we are working to review our existing policies and procedures regarding our third-party vendors, and are working with Blackbaud to evaluate additional measures and safeguards to protect against this type of incident in the future. We will also be notifying state and federal regulators, as required.

0000001



What You Can Do. We encourage you to review the enclosed *Steps You Can Take to Help Protect Your Information*. We have also arranged for complimentary credit monitoring and identity restoration services through Experian. Instructions on how to enroll in these services is included in the enclosed *Steps You Can Take to Help Protect Your Information*. There you will also find general information on what you can do to help protect your personal information.

For More Information. We understand that you may have questions about the Blackbaud incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at (877) 716-4442 Monday through Friday from 8 a.m. to 10 p.m. CST, and Saturday and Sunday from 10 a.m. to 7 p.m. CST. You may also write to Kohl Children's Museum at 2100 Patriot Boulevard, Glenview, Illinois, 60026.

We sincerely regret any inconvenience or concern this incident has caused.

Sincerely,

A handwritten signature in black ink, appearing to read "W. Sanders", written in a cursive style.

William Sanders

Vice President of Business Affairs & CFO

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Activate Your Complimentary Identity Monitoring

To help protect your identity, we are offering a complimentary one-year membership of Experian's® IdentityWorksSM. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you enroll by: November 30, 2020 (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your activation code: ABCDEFGHI

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at (877) 716-4442 by November 30, 2020. Be prepared to provide engagement number DB21911 as proof of eligibility for the identity restoration services by Experian.

Monitor Accounts

In general, we encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian

P.O. Box 9554
Allen, TX 75013
1-888-397-3742

www.experian.com/freeze/center.html

TransUnion

P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872

www.transunion.com/credit-freeze

Equifax

P.O. Box 105788
Atlanta, GA 30348-5788
1-800-685-1111

www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

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, provide 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.);
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.

0000001



As an alternative to a security freeze, you have the right to place an initial or extended “fraud alert” on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian

P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion

P.O. Box 2000
Chester, PA 19016
1-800-680-7289
www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax

P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008
www.equifax.com/personal/credit-report-services

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For New York residents, the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; and <https://ag.ny.gov/>.