17944

Honolulu Museum of Art
C/O IDX
10300 SW Greenburg Rd. Suite 570
Portland, OR 97223

To Enroll, Please Call:
1-800-939-4170
Or Visit: https://app.idx.us/account-creation/protect
Enrollment Code:
<<XXXXXXXX>>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

October 23, 2020

Re: Notification of Data Security Incident

Dear <<FirstName>> <<LastName>>,

As a member of the Honolulu Museum of Art Family, we wanted to let you know about a data security incident experienced by Blackbaud, Inc., a third-party service provider for the Museum, which may have involved some of your information. Because we appreciate the sensitive nature of this information, we want to keep you informed about what occurred. This letter contains information about the incident and provides steps that you can take to protect it.

What Happened: On July 16, 2020, Blackbaud informed us that it had experienced a data security incident that may have involved information pertaining to certain of our vendors. Upon learning of the incident, we immediately engaged our own cybersecurity experts and launched an investigation to determine what happened and what information may have been impacted. Through the course of our investigation, we learned that between February 7, 2020, and May 20, 2020, an unauthorized third party gained access to Blackbaud's servers where backup files for our vendor information were stored. Our investigation determined that some of your information was contained in those backup files. Blackbaud has informed us that it has no reason to believe that any information in the files has been or will be misused or will otherwise be made available publicly.

What Information Was Involved: The incident may have involved the following information: your first and last name, address, and social security number.

What We Are Doing: As soon as we learned of the incident, we engaged our own cybersecurity experts and launched an investigation. We also worked with Blackbaud to obtain additional information regarding the incident, to confirm that your information was not misused, and to ensure that Blackbaud took steps to further protect your information going forward. We also confirmed that the incident was reported to the Federal Bureau of Investigation, and we will offer the FBI whatever assistance is needed. In addition, we are notifying you of the incident and providing you with steps you can take to protect your personal information. Finally, out of an abundance of caution, we are now offering you complimentary credit monitoring and identity protection services. This monitoring will be provided through a leading national identity protection firm, IDX. These services include:

SINGLE BUREAU CREDIT MONITORING - Monitoring of credit bureau for changes to the member's credit file such as new credit inquires, new accounts opened, delinquent payments, improvements in the member's credit report, bankruptcies, court judgments and tax liens, new addresses, new employers, and other activities that affect the member's credit record.

CYBERSCAN™ - Dark Web monitoring of underground websites, chat rooms, and malware, 24/7, to identify trading or selling of personal information like SSNs, bank accounts, email addresses, medical ID numbers, driver's license numbers, passport numbers, credit and debit cards, phone numbers, and other unique identifiers.

IDENTITY THEFT INSURANCE - Identity theft insurance will reimburse members for expenses associated with restoring their identity should they become a victim of identity theft. If a member's identity is compromised, the policy provides coverage for up to $1,000,000, with no deductible, from an A.M. Best "A-rated" carrier. Coverage is subject to the terms, limits, and/or exclusions of the policy.

FULLY-MANAGED IDENTITY RECOVERY – IDX fully-managed recovery service provides restoration for identity theft issues such as (but not limited to): account creation, criminal identity theft, medical identity theft, account takeover, rental application, tax fraud, benefits fraud, and utility creation. This service includes a complete triage process for affected individuals who report suspicious activity, a personally assigned IDCare Specialist to fully manage restoration of each case, and expert guidance for those with questions about identity theft and protective measures.

What You Can Do: We recommend that you remain vigilant by reviewing account statements and monitoring your free credit reports. We also recommend that you activate your complimentary IDX service. To activate this service, call 1-800-939-4170 or go to https://app.idx.us/account-creation/protect and use the enrollment code at the top of this letter. You must activate by January 23, 2021. We also recommend that you review the guidance included with this letter about how to ensure your information is protected, in particular contacting your financial institution to ensure that your account is protected.

For More Information: If you have any questions about this letter, please call 1-800-939-4170 between 3 a.m. and 3 p.m. Hawaiian Time. You may also consult the resources included on the following page, which provide information about how to protect your personal data.

***

The security of your information is a top priority for the Museum and we take this responsibility very seriously. We apologize for any inconvenience this may have caused.

Sincerely,

Tania Ginoza

Tania Ginoza
Chief Financial Officer
Honolulu Museum of Art

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 105851	P.O. Box 105281
Chester, PA 19016	Allen, TX 75013	Atlanta, GA 30348	Atlanta, GA 30348
1-877-322-8228	1-888-397-3742	1-800-525-6285	1-877-322-8228
www.transunion.com	www.experian.com	www.equifax.com	www.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. Residents of Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

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	www.oag.state.md.us	www.ncdoj.gov	www.riag.ri.gov
www.ftc.gov/idtheft	1-888-743-0023	1-877-566-7226	1-401-274-4400
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.