LEWIS BRISBOIS BISGAARD & SMITH LLP

Donna Maddux
888 SW Fifth Avenue, Suite 900
Portland, Oregon 97204-2025
Donna.Maddux@lewisbrisbois.com
Direct: 971.334.7001

File No. 49905.19

December 30, 2021

VIA ONLINE PORTAL

Attorney General Aaron Frey
Office of the Attorney General
Consumer Protection Division
Security Breach Notification
111 Sewall Street, 6th Floor
Augusta, ME 04330

Re: **Notice of Data Security Incident**

Dear Attorney General Frey:

Lewis Brisbois Bisgaard & Smith LLP represents Municipal Art Society of New York ("MAS"), a non-profit located in New York, New York in connection with a recent data security incident that may have affected the information of certain Maine residents.

1. NATURE OF THE SECURITY INCIDENT

MAS experienced a network disruption on June 22, 2021. MAS immediately took steps to secure their environment and engaged cybersecurity experts to assist with an investigation. The investigation determined that an unknown actor gained access to and obtained data from the MAS network without authorization.

MAS undertook a review of the information that could have potentially been accessed as a result of the incident. On December 17, 2021, MAS determined that information related to its customers and employees, including the personal information of 1 Maine resident (deceased), was potentially impacted. The information potentially accessed without authorization may have included the first and last name, and Social Security Number. To date, MAS has no evidence that any potentially impacted information has been misused in conjunction with this incident.

2. NUMBER OF MAINE RESIDENTS AFFECTED

MAS notified the 1 Maine resident of this data security incident via first class U.S. mail on December 30, 2021. A sample copy of the notification letter sent to the affected individuals is attached.

3. STEPS TAKEN RELATING TO THE INCIDENT

MAS implemented additional security features to reduce the risk of a similar incident occurring in the future. MAS also reported this incident to the Federal Bureau of Investigation and will provide whatever cooperation is necessary to attempt to hold the perpetrators of this incident accountable, if possible.

While MAS has no indication that the information has been misused, it nonetheless is providing individuals with information about steps that they can take to help protect their personal information. As a further precaution, MAS is also offering Maine consumers one year of complimentary credit and identity monitoring services through IDX. This product helps detect possible misuse of personal information and provides consumers whose information may have been accessed without authorization with identity protection support.

4. CONTACT INFORMATION

MAS is committed to protecting the security of the personal information in their possession. Please feel free to contact me at Donna.Maddux@lewisbrisbois.com or by phone at 971-334-7001 if you have any further questions.

Very truly yours,

Donna Maddux of
LEWIS BRISBOIS BISGAARD & SMITH LLP

DM
Enclosure: Sample Consumer Notification Letter

The Municipal Art Society of New York
MASNYC

<<DATE>>

<<First Name>> <<Last Name>>
<<Address 1>>
<<Address 2>>

<<City>><<State>><<Zip>>

Subject: Notice of Data Security <<variable text -[Breach for CA - Incident for all other states] >>

Dear <FNAME> <LNAME:

Municipal Art Society of New York ("MAS") is writing to inform you of a data security incident which may have involved some of your personal information. At MAS, we take the privacy and security of the personal information we maintain very seriously. That is why we are writing to provide you with information about this incident and about steps that you can take to help protect your personal information, including an offer of complimentary credit monitoring and identity protection services.

What Happened: On June 22, 2021, MAS experienced a network disruption. We immediately took steps to secure our environment and engaged cybersecurity experts to assist us with an investigation. The investigation determined that an unknown actor gained access to and may have obtained data from the MAS network without authorization. On December 17, 2021, we determined that some of your personal information may have been involved in the incident. We currently have no reason to believe your information was misused as a result of this incident, only that it was potentially accessed or acquired.

What Information Was Involved: The information may have involved your name and your <<variable text >>.

What We Are Doing: As soon as we discovered the incident, we took the steps referenced above. We also implemented additional security features to reduce the risk of a similar incident occurring in the future. We reported this incident to the Federal Bureau of Investigation and will provide whatever cooperation is necessary to attempt to hold the perpetrators of this incident accountable, if possible. We are further notifying you of this event and advising you about steps you can take to help protect your information.

Additionally, we are offering you complimentary credit monitoring and identity protection services for <<variable text >> through IDX, a national leader in identity protection services. The IDX services, which are free to you upon enrollment, include a <<variable text >> year subscription for the

following: single bureau credit monitoring, CyberScan dark web monitoring, fully-managed identity recovery services, and $1 million in identity theft insurance coverage. With this protection, IDX will help you resolve issues if your identity is compromised.

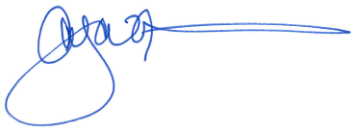
What You Can Do: We recommend that you review the guidance included with this letter about how to protect your personal information. In addition, we recommend enrolling in the complimentary identity protection services being offered through IDX to further protect your personal information. To receive credit monitoring services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

To enroll in the complimentary identity protection services provided through IDX, please call 1-800-939-4170 Monday through Friday from [IDX please insert time period in EST] or visit https://app.idx.us/account-creation/protect and insert the Enrollment Code provided above. Please note the deadline to enroll in these complimentary services is [Enrollment Deadline]. You will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

For More Information. If you have questions about the complimentary services or need assistance, please contact customer service for IDX at 1-800-939-4170. IDX representatives are available Monday through Friday from[IDX please insert time period in EST]. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Sincerely,



Elizabeth Goldstein
President, Municipal Art Society of New York

ADDITIONAL 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 monitoring free credit reports closely for errors and by taking other steps appropriate to protect accounts, including promptly changing passwords. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained for remediation assistance or contact a remediation service provider. 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). You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Ave, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.consumer.ftc.gov, www.ftc.gov/idtheft.

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:

- *Equifax*, P.O. Box 740241, Atlanta, GA 30374, 1-800-525-6285, www.equifax.com.
- *Experian*, P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com.
- *TransUnion*, P.O. Box 1000, Chester, PA 19016, 1-800-916-8800, www.transunion.com.

Fraud Alerts: There are two kinds of general fraud alerts you can place on your credit report—an initial alert and an extended alert. You may want to consider placing either or both fraud alerts 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. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and provide the appropriate documentary poof. An extended fraud alert is also free and will stay on your credit report for seven years. 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. Military members may also place an Active Duty Military Fraud Alert on their credit reports while deployed. An Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment

Credit or Security Freezes: Under U.S. law, you have the right to put a credit freeze, also known as a security freeze, on your credit file, for up to one year at no cost. The freeze 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 fee to place or lift a security freeze. For information and instructions on how to place a security freeze, contact any of the credit reporting agencies or the Federal Trade Commission identified above. 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. After receiving your freeze request, each credit bureau will provide you with a unique PIN or password. Keep the PIN or password in a safe place as you will need it if you choose to lift the freeze.

A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or via phone, a credit bureau must lift the credit freeze within an hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after receiving your request.

IRS Identity Protection PIN: You can obtain an identity protection PIN (IP PIN) from the IRS that prevents someone else from filing a tax return using your Social Security number. The IP PIN is known only to you and the IRS and helps the IRS verify your identity when you file your electronic or paper tax return. You can learn more and obtain your IP PIN here: https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin.

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include the right 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. 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.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state attorney general about fraud alerts, security freezes, and 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.

Additional information:

District of Columbia: The Office of the Attorney General for the District of Columbia can be reached at 400 6th Street, NW, Washington, DC 2000; (202) 727-3400; oag@dc.gov .gov

Maine: Maine Attorney General can be reached at: 6 State House Station Augusta, ME 04333; 207-626-8800; https://www.maine.gov/ag/.

Maryland: Maryland Attorney General can be reached at: 200 St. Paul Place Baltimore, MD 21202; 1-888-743-0023; oag@state.md.us or IDTheft@oag.state.md.us

MAS: MAS can be reached via mail at 488 Madison Ave, Suite 1900, New York, NY 10022 and via phone (212) 935–3960.

North Carolina: North Carolina Attorney General's Office, Consumer Protection Division, can be reached at: 9001 Mail Service Center Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; www.ncdoj.gov

New York: New York Attorney General can be reached at: Bureau of Internet and Technology Resources, 28 Liberty Street, New York, NY 10005, 1-212-416-8433, https://ag.ny.gov/.

Rhode Island: [#] Rhode Island resident may have been affected by the Incident. Rhode Island Attorney General can be reached at: 150 South Main Street Providence, RI 02903, http://www.riag.ri.gov.

Vermont: Vermont Attorney General's Office can be reached at: 109 State Street, Montpelier, VT 05609; Phone (802) 828-3171; Email: ago.info@vermont.gov.

Washington D.C.: Washington D.C. Attorney General can be reached at: 441 4th Street, NW Washington, DC 20001, 1-202-727-3400, oag.dc.gov.