SHAWE
ROSENTHAL LLP

One South Street
Suite 1800
Baltimore, MD 21202
P: 410-752-1040
F: 410-752-8861

shawe.com

Electronic Letterhead

VIA ELECTRONIC MAIL

May 11, 2020

Mark J. Swerdlin
swerdlin@shawe.com
410-843-3468

Consumer Protection Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301
E-Mail: DOJ-CPB@doj.nh.gov

Re: Data Breach Notification

To Whom it May Concern:

My law firm represents The Baltimore Museum of Art ("BMA"). I am writing to notify you of a data security event involving the exposure of certain personal information described in more detail below. Please be aware that BMA takes the security of personal information in its control seriously and has taken significant steps intended to prevent a similar event in the future.

I. Nature of the Security Event

At some point between April 27, 2020 and April 28, 2020, certain BMA email accounts were accessed by an unauthorized third party. The third party used these user's login credentials to access their BMA email accounts. The third party then used one of the BMA accounts to send out phishing emails. The emails appeared to contain OneDrive attachments, but directed users to spoof websites that asked users to provide their Office 365 login credentials, as well as credentials for other email providers. From there, the third party attempted to run a fake payroll, with fictitious employees, though the activity was stopped by Deluxe Payroll, the BMA's payroll provider. There is no evidence thus far of any tampering with anyone's personal information.

BMA immediately initiated a forced logout for the affected employees on all devices. The passwords for these employees were reset, and multi-factor authentication was added to those users' accounts. BMA's IT team continues to work with Microsoft support on tracing the exact time the accounts were exposed as well as continuing to update Outlook security across all applications.

SHAWE ROSENTHAL LLP

II. Steps Taken or Planned to be Taken Related to the Security Event

BMA is offering impacted individuals a complimentary one-year membership in credit monitoring and theft protection services through NortonLifeLock, Inc., and its **LifeLock Defender™ Choice** solution. Details about those services and enrollment instructions are contained in BMA's notification email and letter to impacted individuals.

BMA's IT team is working with all staff to update the security on their email accounts. IT is also working to improve its email filtering. Additional staff security training will be scheduled in upcoming weeks.

III. Number of New Hampshire Residents Affected

On May 5, 2020, BMA emailed all staff and former staff, which includes one (1) New Hampshire resident, in substantially the same form as the email attached as Exhibit 1. On May 7, 2020, BMA sent a letter to all staff and former staff, in substantially the same form as the letter attached as Exhibit 2.

IV. Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact me at 410-843-3468 or mjs@shawe.com.

Sincerely,

SHAWE ROSENTHAL LLP

/s/

Mark J. Swerdlin

MJS/wam
Enclosures

#812573

Dear Colleagues,

We are writing to tell you about a data security incident that may have exposed certain of your personal information to unauthorized intruders. This is a detailed message so please read it carefully and know that we take this matter very seriously and are doing all we can to protect your personal information.

At some point between Monday, April 27, 2020 and Tuesday, April 28, 2020, certain BMA email accounts were accessed by an unauthorized third party. The third party used these user's login credentials to access their BMA email accounts, though how the third party obtained the passwords remains unclear. The third party then used one of the BMA accounts to send out phishing emails. The emails appeared to contain OneDrive attachments, but directed users to spoof websites that asked users to provide their Office 365 login credentials, as well as credentials for other email providers. From there, the third party attempted to run a fake payroll, with fictitious employees, though the activity was stopped by Deluxe Payroll, the BMA's payroll provider.

We have worked with Deluxe to audit the activity in the payroll system. While there is NO evidence that anyone's personal information was tampered with and Deluxe feels strongly that the third party used the access only to add and pay fraudulent (i.e., fictitious) employees, they did have access to all of the information in the payroll system.

We take the protection and proper use of your personal information very seriously. For this reason, in addition to explaining what happened, we are advising you about what we are doing to protect you from fraud and identity theft.

What We Are Doing to Protect You

The BMA immediately initiated a forced logout for the affected employees on all devices. The passwords for these employees were reset, and multi-factor authentication was added to the users' accounts (see below for security upgrades for other employees). The BMA's IT team continues to work with Microsoft support on tracing the exact time the accounts were exposed as well as continuing to update Outlook security across all applications.

We are also notifying the Maryland Attorney General's office, the FBI, and the IRS of this cyber breach and sharing with them all of the information we have regarding the breach and how we are responding to it.

We understand that incidents like this will cause a multitude of concerns. In order to help relieve any such concerns and restore confidence following this incident, we have contracted with NortonLifeLock, Inc., to make available to all of you its **LifeLock Defender™ Choice** solution for one year. This service is offered to all of you at no cost. As you may be aware, NortonLifeLock, Inc. is an industry leader in providing credit and identity theft monitoring and remediation services and products. Their incident response team has extensive experience in assisting people who have sustained an unintentional exposure of their personal information.

LifeLock Defender™ Choice is specifically designed to protect your personal information as well as your financial standing and personal identity. In the unlikely event that you are impacted by this incident, LifeLock will take all steps necessary to respond to, remediate and rectify the situation. **Letters with all**

of the necessary enrollment information will be mailed to you by the end of this week. Once you have completed the LifeLock enrollment process, the service will be in effect. Your LifeLock Defender™ Choice membership includes:

- Primary Identity Alert System
- 24/7 Live Member Support
- Dark Web Monitoring
- Norton™ Security Deluxe (90 Day Free Subscription)
- Stolen Funds Reimbursement up to $25,000
- Personal Expense Compensation up to $25,000
- Coverage for Lawyers and Experts up to $1 million
- U.S.-Based Identity Restoration Team
- One-Bureau Credit Monitoring
- Annual One-Bureau Credit Report & Credit Score

We are also providing you with the attached Recommended Steps to help Protect your Information, which identifies other measures that you can take to protect yourself from identity theft. It also includes contact information for the Federal Trade Commission, state Attorneys General, and the three major credit bureaus, should you wish to contact them as well.

New IT Policies
The IT team is working with all staff to update the security on their email accounts (please refer to the schedule [redacted] sent on 4/30/2020). Multi-factor authentication is being applied to all email accounts, so users accessing email through a web browser will always need to enter both a password and a six-digit code they will receive by text. IT is also working to improve its Office 365 Advanced Threat Protection email filtering with the hope that fewer phishing emails land in user inboxes. Additional staff security training will be scheduled in upcoming weeks.

What You Can Do
In addition to utilizing the LifeLock solution, which we strongly encourage you to take advantage of, we also caution you to be vigilant in protecting your personal information. By way of example, you might change all of your website and computer passwords, check your bank and credit card statements to see if there have been any unusual or unauthorized transactions or activity, and take similar remedial measures that only you can do, as suggested on the attached document.

IMMEDIATE NEXT STEPS
While we do not believe that any personal account information was altered, If you would like to stop your direct deposit for this week's pay date, and receive a paper check instead, please let [redacted] or [redacted] know by 10 am on Wednesday, May 6th. This paper check will be mailed to your home address or we can provide you with instructions on picking it up at the museum. Going forward, all direct deposit changes will be made via signed hard copy of the BMA's direct deposit form. If you elect to delete your banking information for this pay, you will continue to receive a paper check until we receive a signed copy of this form.

Please also login to mypaycenter.com **by 10 am, Wednesday, May 6**, and make sure that we have your most current address on file so that we can ensure that the LifeLock enrollment information reaches you in a timely manner.

Please rest assured that our employees' and their families' well-being and the security of your personal information are our highest priorities. We apologize for any inconvenience this incident may cause you and thank you for your understanding and patience.

If you have any questions or need additional information about this notice, please reach out to [redacted] She will not be able to help with enrolling in NortonLifeLock, Inc., however, as this is your own personal protection account and you will need to follow the instructions received in the letter.

Please let [redacted] or [redacted] r know if you do not receive an enrollment letter from NortonLifeLock, Inc. by Wednesday, May 13, 2020.

<<Client First Name>> <<Client Last Name>> **<<Date>> (Format: Month Day, Year)**
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip Code>>

Notice of Data Breach

Dear **<<First Name>>** **<<Last Name** >>,

We are writing to tell you about a data security incident that may have exposed certain of your personal information to unauthorized intruders. This is a detailed letter so please read it carefully and know that we take this matter very seriously and are doing all we can to protect your personal information.

What Happened and What Information was Involved

At some point between April 27, 2020 and April 28, 2020, certain BMA email accounts were accessed by an unauthorized third party. The third party used these user's login credentials to access their BMA email accounts. The third party then used one of the BMA accounts to send out phishing emails. The emails appeared to contain OneDrive attachments, but directed users to spoof websites that asked users to provide their Office 365 login credentials, as well as credentials for other email providers. From there, the third party attempted to run a fake payroll, with fictitious employees, though the activity was stopped by Deluxe Payroll, the BMA's payroll provider. There is no evidence thus far of any tampering with anyone's personal information.

What We Are Doing to Protect You

The BMA immediately initiated a forced logout for the affected employees on all devices. The passwords for these employees were reset, and multi-factor authentication was added to the users' accounts (see below for security upgrades for other employees). The BMA's IT team continues to work with Microsoft support on tracing the exact time the accounts were exposed as well as continuing to update Outlook security across all applications.

We are also notifying the Maryland Attorney General's office, the FBI, the IRS, and any other required entities of this cyber breach and sharing with them all of the information we have regarding the breach and how we are responding to it.

In order to help relieve any such concerns and restore confidence following this incident, we have contracted with NortonLifeLock, Inc., to make available at no cost to you for <<MEMBERSHIP TERM>> months, its **LifeLock Defender™ Choice** solution. As you may be aware, **NortonLifeLock, Inc.** is an industry leader in providing credit and identity theft monitoring and remediation services and products. Their incident response team has extensive experience in assisting people who have sustained an unintentional exposure of their personal information.

LifeLock Defender™ Choice is specifically designed to protect your personal information as well as your financial standing and personal identity. In the unlikely event that you are impacted by this incident, **NortonLifeLock** will take all steps necessary to respond to, remediate and rectify the situation.

To activate your membership online and get protection at no cost to you:

1. In your web browser, go directly to **www.LifeLock.com**. Click on the yellow "**START MEMBERSHIP**" button *(do not attempt registration from a link presented by a search engine)*.
2. You will be taken to another page where, below the FOUR protection plan boxes, you may enter the **Promo Code:**

<<PROMO CODE>> and click the "**APPLY**" button.

3. On the next screen, enter your **Member ID: <<MEMBER ID>>** and click the "**APPLY**" button.
4. Your complimentary offer is presented. Click the red "**START YOUR MEMBERSHIP**" button.
5. Once enrollment is completed, you will receive a confirmation email (be sure to **follow ALL directions** in this email).

Alternatively, you may activate your membership over the phone. To do so, please call: 1-800-899-0180.

You have until August 15, 2020 to enroll in this service.

Once you have completed the LifeLock enrollment process, the service will be in effect. Your <<MEMBERSHIP TERM>> month **LifeLock Defender™ Choice** membership includes:

- ✓ Primary Identity Alert System†
- ✓ 24/7 Live Member Support
- ✓ Dark Web Monitoring**
- ✓ Norton™ Security Deluxe[2] (90 Day Free Subscription)
- ✓ Stolen Funds Reimbursement up to $25,000 †††
- ✓ Personal Expense Compensation up to $25,000 †††
- ✓ Coverage for Lawyers and Experts up to $1 million †††
- ✓ U.S.-Based Identity Restoration Team
- ✓ One-Bureau Credit Monitoring[1]**
- ✓ Annual One-Bureau Credit Report & Credit Score[1]**

  The credit score provided is a VantageScore 3.0 credit score based on Equifax data. Third parties use many different types of credit scores and are likely to use a different type of credit score to assess your creditworthiness.

[1] If your plan includes credit reports, scores, and/or credit monitoring features ("Credit Features"), two requirements must be met to receive said features: (i) your identity must be successfully verified with Equifax; and (ii) Equifax must be able to locate your credit file and it must contain sufficient credit history information. IF EITHER OF THE FOREGOING REQUIREMENTS ARE NOT MET YOU WILL NOT RECEIVE CREDIT FEATURES FROM ANY BUREAU. If your plan also includes Credit Features from Experian and/or TransUnion, the above verification process must also be successfully completed with Experian and/or TransUnion, as applicable. If verification is successfully completed with Equifax, but not with Experian and/or TransUnion, as applicable, you will not receive Credit Features from such bureau(s) until the verification process is successfully completed and until then you will only receive Credit Features from Equifax. Any credit monitoring from Experian and TransUnion will take several days to begin after your successful plan enrollment.
No one can prevent all identity theft or cybercrime. † LifeLock does not monitor all transactions at all businesses.
[2]Norton Security Online provides protection against viruses, spyware, malware, and other online threats for up to 5 PCs, Macs, Android devices. Norton account features not supported in this edition of Norton Security Online. As a result, some mobile features for Android are not available such as anti-theft and mobile contacts backup. iOS is not supported.
** These features are not enabled upon enrollment. Member must take action to get their protection.
††† Reimbursement and Expense Compensation, each with limits of up to $25,000 for Defender Choice. And up to $1 million for coverage for lawyers and experts if needed, for all plans. Benefits provided by Master Policy issued by United Specialty Insurance Company (State National Insurance Company, Inc. for NY State members). Policy terms, conditions and exclusions at: LifeLock.com/legal.

We are also providing you with the attached Recommended Steps to help Protect your Information, which identifies other measures that you can take to protect yourself from identity theft. It also includes contact information for the Federal Trade Commission, state Attorney General, and the three major credit bureaus, should you wish to contact them as well.

What You Can Do

In addition to utilizing the LifeLock solution, which we strongly encourage you to take advantage of, we also caution you to be vigilant in protecting your personal information. By way of example, you might change all of your website and computer passwords, check your bank and credit card statements to see if there have been any unusual or unauthorized transactions or activity, and take similar remedial measures that only you can do, as suggested on the attached document.

Please rest assured that our employees' and their families' well-being and the security of their personal information are our highest priorities. We apologize for any inconvenience this incident may cause you and thank you for your understanding and patience.

For More Information

If you have any questions or need additional information about this Notice, please contact Kim Bountress, Senior Director of Human Resources, at 443-573-1717 or kbountress@artbma.org. She will not be able to help with enrolling in NortonLifeLock, Inc., however, as this is your own personal protection account and you will need to follow the instructions received in this letter.

Sincerely,

Christine Dietze, Chief Operating Officer

Recommended Steps to Help Protect Your Information

It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

You can obtain information from the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft. The FTC can be reached at:

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

Fraud Alerts: You can place fraud alerts with the three major credit bureaus by phone and also via their websites. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three credit bureaus is below.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, or regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security
number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. The consumer reporting agency may charge a small fee to place, life, or remove a freeze, but is free if you are a victim of identity theft or the spouse of a victim of identity theft, and you have submitted a valid police report relating to the identity theft incident to the consumer reporting agency.

You may obtain a security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
www.freeze.equifax.com
800-525-6285

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
www.experian.com/freeze
888-397-3742

TransUnion (FVAD)
P.O. Box 2000
Chester, PA 19022
http://freeze.transunion.com
800-680-7289

If you live in Maryland, please read the additional notice below that applies to you:

You can obtain information from your state's Attorney General Office about steps you can take to prevent identity theft.

Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023
www.marylandattorneygeneral.gov