



MULLEN  
COUGHLIN LLC  
ATTORNEYS AT LAW

STATE OF NH  
DEPT OF JUSTICE  
2019 APR 16 PM 12:03

Jeffrey J. Boogay  
Office: 267-930-4784  
Fax: 267-930-4771  
Email: jboogay@mullen.law

1275 Drummers Lane, Suite 302  
Wayne, PA 19087

April 12, 2019

**VIA U.S. MAIL**

Attorney General Gordon J. MacDonald  
Office of the New Hampshire Attorney General  
Attn: Security Breach Notification  
33 Capitol Street  
Concord, NH 03301

**Re: Notice of Data Event**

Dear Attorney General MacDonald:

We represent Manhattan School of Music ("MSM"), 130 Claremont Avenue, New York, New York, 10027, and write to notify your Office of a recent incident that may affect the privacy of certain personal information of one (1) New Hampshire resident. By providing this notice, MSM does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data incident notification statute, or personal jurisdiction.

**Nature of the Data Event**

On March 7, 2019, MSM discovered a former employee forwarded certain MSM emails received while employed with MSM to her personal email account. As this was a violation of MSM policy, MSM immediately launched an investigation to determine the content of the forwarded emails and to determine why the former employee forwarded these emails. While the forwarding of these emails does not appear to be ill-intended, MSM did determine that some emails contained financial information received related to donations. Although MSM have no evidence to suggest misuse of this information, it is nonetheless providing notice to individuals out of an abundance of caution because their financial information was present in the forwarded emails. The financial information included personal checks.

**Notice to New Hampshire Resident**

MSM provided written notice to the individuals with information within the emails including one (1) New Hampshire resident, on April 12, 2019. Written notice will be provided in substantially the same form as the letter attached here as *Exhibit A*.

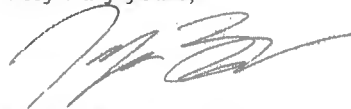
### **Other Steps Taken and To Be Taken**

Upon learning of this incident, MSM quickly took steps to review the forwarded emails to confirm the information contained therein and identify those individuals whose information was present. MSM contacted the former employee; however, she refused to cooperate with MSM's investigation. Although MSM is unaware of any actual or attempted misuse of the financial information in the forwarded emails, MSM is providing impacted individuals with access to 1 year of free credit monitoring and identity theft protection services through Kroll. MSM is also providing guidance on how to better protect against identity theft and fraud, including information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

### **Contact Information**

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 267-930-4784.

Very truly yours,



Jeffrey J. Boogay of  
MULLEN COUGHLIN LLC

JJB/mep  
Enclosure

# **EXHIBIT A**

# **M** Manhattan School of Music

130 CLAREMONT AVENUE, NEW YORK, NY 10027-4698



## **Notice of Data Breach**

Dear [REDACTED]:

Manhattan School of Music (“MSM”) writes to notify you of an incident that may affect the security of some of your financial information provided to MSM. We take this incident very seriously and write to provide you with details of the incident, our response, and steps you can take to protect your information, should you feel it is appropriate to do so.

***What Happened?*** On March 7, 2019, MSM discovered a former employee blind-copied certain MSM emails received to their personal email account while employed with MSM. As this was a violation of MSM policy, we immediately launched an investigation to determine the content of the blind-copied emails and to determine why the former employee took these actions. While the blind-copying of these emails does not appear to be ill-intended, we did determine that some emails contained financial information received related to donations. Although we have no evidence to suggest misuse of this information, we are nonetheless providing you notice out of an abundance of caution because your financial information was present in the blind-copied emails.

***What Information Was Involved?*** Our investigation confirmed the personal information present in the impacted email account includes your name, checking account number and routing number.

***What Are We Doing?*** The security of the information provided to us is among our highest priorities, and we have strict security measures in place to protect information in our care. Upon learning of this incident, we quickly took steps to review the blind-copied emails to confirm the information contained therein and identify those individuals whose information was present. Again, in an abundance of caution, we are also notifying affected individuals so that you may take steps to best protect your personal information, should you feel it is appropriate to do so. Although we are unaware of any actual or attempted misuse of your personal information as a result of this incident, we arranged to have Kroll Cyber Security protect your identity for one year at no cost to you as an added precaution.

***What Can You Do?*** You may review the information contained in the attached “Steps You Can Take to Protect Against Identity Theft and Fraud.” You may also enroll to receive the identity protection services we are making available to you. We will cover the cost of this service; however, you will need to enroll yourself in this service.

***For More Information.*** We recognize that you may have questions not addressed in this letter. If you have additional questions, please call [REDACTED], Monday through Friday, 9:00 a.m. to 5:00 p.m., ET. You may also write to [REDACTED] at Manhattan School of Music, 130 Claremont Avenue, New York, NY, 10027. We sincerely regret any inconvenience this incident may cause you and greatly appreciate your support.

Sincerely,



## STEPS YOU CAN TAKE TO PROTECT AGAINST IDENTITY THEFT AND FRAUD

We have secured the services of Kroll to provide identity monitoring at no cost to you for 12 months. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit [krollbreach.idmonitoringservice.com](http://krollbreach.idmonitoringservice.com) to activate and take advantage of your identity monitoring services.

You have until July 5, 2019 to activate your identity monitoring services.

Membership Number: [REDACTED]

To receive credit services by mail instead of online, please call [REDACTED]. Additional information describing your services is included with this letter. You may also contract Kroll directly at 1-866-775-4209, Monday through Friday from 8:00 a.m. to 5:30 p.m. CT.

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](http://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:

<b>Experian</b> PO Box 9554 Allen, TX 75013 1-888-397-3742 <a href="http://www.experian.com/freeze/center.html">www.experian.com/freeze/center.html</a>	<b>TransUnion</b> P.O. Box 2000 Chester, PA 19016 1-888-909-8872 <a href="http://www.transunion.com/credit-freeze">www.transunion.com/credit-freeze</a>	<b>Equifax</b> PO Box 105788 Atlanta, GA 30348-5788 1-800-685-1111 <a href="http://www.equifax.com/personal/credit-report-services">www.equifax.com/personal/credit-report-services</a>
---	---	---

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.

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 2002  
Allen, TX 75013  
1-888-397-3742

[www.experian.com/fraud/center.html](http://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](http://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](http://www.equifax.com/personal/credit-report-services)

Although we have no reason to believe that your personal information has been used to file fraudulent tax returns, you can contact the IRS at [www.irs.gov/Individuals/Identity-Protection](http://www.irs.gov/Individuals/Identity-Protection) for helpful information and guidance on steps you can take to address a fraudulent tax return filed in your name and what to do if you become the victim of such fraud. You can also visit [www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft](http://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft) for more 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](http://www.identitytheft.gov), 1-877-ID-THEFT (1-877-438-4338); 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.

## TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services<sup>1</sup> from Kroll:

### **Triple Bureau Credit Monitoring and Single Bureau Credit Report**

Your current credit report is available for you to review. You will also receive alerts when there are changes to your credit data at any of the three national credit bureaus—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

### **Web Watcher**

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

### **Public Persona**

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you'll receive an alert.

### **Quick Cash Scan**

Quick Cash Scan monitors short-term and cash-advance loan sources. You'll receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

### **\$1 Million Identity Fraud Loss Reimbursement**

Reimburses you for out-of-pocket expenses totaling up to \$1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

### **Fraud Consultation**

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

### **Identity Theft Restoration**

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

<sup>1</sup> Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. To receive credit 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.