



MULLEN  
COUGHLIN<sub>LLC</sub>  
ATTORNEYS AT LAW

RECEIVED

FEB 05 2021

CONSUMER PROTECTION

Angelina W. Freind  
Office: 267-930-4782  
Fax: 267-930-4771  
Email: [afreind@mullen.law](mailto:afreind@mullen.law)

426 W. Lancaster Ave, Suite 200  
Devon, PA 19333

January 29, 2021

**INTENDED FOR ADDRESSEE(S) ONLY**

**VIA U.S. MAIL**

Consumer Protection Bureau  
Office of the New Hampshire Attorney General  
33 Capitol Street  
Concord, NH 03301

**Re: Notice of Data Event**

Dear Sir or Madam:

We represent San Francisco Conservatory of Music (“SFCM”) located at 50 Oak Street, San Francisco, CA 94102, and write to notify your office of an incident that occurred at SFCM’s third-party vendor, Blackbaud, Inc. (“Blackbaud”). The incident may affect the security of certain personal information relating to approximately two (2) New Hampshire residents. The investigation into this incident is ongoing, and this notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, SFCM does not waive any rights or defenses regarding the applicability of New Hampshire law, the New Hampshire data breach notification statute, or personal jurisdiction.

**Nature of the Data Event**

SFCM received information from Blackbaud that it experienced an attempted ransomware incident that impacted certain Blackbaud systems. Blackbaud reported the incident to law enforcement and worked with forensic investigators to determine the nature and scope of the incident. Blackbaud’s investigation determined that an unknown actor may have accessed or acquired certain Blackbaud customer data. Blackbaud further reported that data was exfiltrated by the threat actor at some point before Blackbaud locked the threat actor out of the environment on May 20, 2020.

SFCM received a supplemental notification from Blackbaud on September 29, 2020, which indicated that this incident impacted personal information related to SFCM. Upon receiving this notification, SFCM immediately commenced an investigation to determine what, if any, sensitive

[Mullen.law](http://Mullen.law)

SFCM data was potentially involved. This investigation included working diligently to obtain further information from Blackbaud to understand the scope of the incident and the data that may have been affected. Using lists of potentially impacted individuals supplied by Blackbaud in October 2020, SFCM reviewed internal records to compare the information provided by Blackbaud and confirm the identities and contact information for individuals whose personal information may have been impacted by this incident. SFCM completed the identity and address research on or about December 11, 2020. Upon completion of the internal review, SFCM worked to prepare a complete list of individuals requiring notice of this event. This final list of affected individuals was completed on or about January 8, 2021.

The investigation determined that the following types of information related to New Hampshire residents may have been accessible within the impacted system: name and Social Security number.

#### **Notice to New Hampshire Residents**

On or around January 29, 2021, SFCM began providing written notice of this incident to potentially affected individuals, including approximately two (2) New Hampshire residents. Written notice is being 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, SFCM moved quickly to investigate and respond, assess the security of SFCM's system, and notify potentially affected individuals. As part of its ongoing commitment to the security of information in its care, SFCM is working to review its existing policies and procedures regarding its third-party vendors, and is working with Blackbaud to evaluate additional measures and safeguards to protect against this type of incident in the future. SFCM is also notifying relevant regulatory authorities of this event, as required by applicable law.

Additionally, SFCM is providing potentially impacted individuals with complimentary credit monitoring and identity protection services for twenty-four (24) months through CyberScout. SFCM is providing potentially affected individuals with 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.

Office of the New Hampshire Attorney General  
January 29, 2021  
Page 3

**Contact Information**

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 267-930-4782.

Very truly yours,

A handwritten signature in black ink, appearing to read 'AF', with a long horizontal flourish extending to the right.

Angelina W. Freind of  
MULLEN COUGHLIN LLC

AWF:mfl  
Enclosure

# Exhibit A



Return Mail Processing Center  
P.O. Box 6336  
Portland, OR 97228-6336

<<Mail ID>>  
<<Name 1>>  
<<Name 2>>  
<<Address 1>>  
<<Address 2>>  
<<Address 3>>  
<<Address 4>>  
<<Address 5>>  
<<City>><<State>><<Zip>>  
<<Country>>

<<Date>>

Re: Notice of Data Breach

Dear <<Name 1>>:

San Francisco Conservatory of Music (“SFCM”) is writing to make you aware of a data privacy event at our third-party vendor, Blackbaud, Inc. (“Blackbaud”), that may affect the privacy of some of your personal information. Blackbaud is a cloud computing provider that offers customer relationship management and financial services tools to organizations, including SFCM. This notice provides information about the Blackbaud incident, SFCM’s response, and resources available to you to help protect your information from possible misuse, should you feel it necessary to do so.

**What Happened?** SFCM received information from Blackbaud that it experienced an attempted ransomware incident that impacted certain Blackbaud systems. Blackbaud reported the incident to law enforcement and worked with forensic investigators to determine the nature and scope of the incident. Blackbaud’s investigation determined that an unknown actor may have accessed or acquired certain Blackbaud customer data. Blackbaud further reported that data was exfiltrated by the threat actor at some point before Blackbaud locked the threat actor out of the environment on May 20, 2020. SFCM received a supplemental notification from Blackbaud on September 29, 2020, that this incident impacted personal information related to SFCM. Upon receiving this notification, SFCM immediately commenced an investigation to determine what, if any, sensitive SFCM data was potentially involved. This investigation included working diligently to obtain further information from Blackbaud to understand the scope of the incident and the data that may have been affected. Using lists of potentially impacted individuals supplied by Blackbaud in October 2020, SFCM reviewed internal records to compare the information provided by Blackbaud with internal records and confirm the identities and contact information for individuals whose personal information may have been impacted by this event. The identity and address research was completed on or about December 11, 2020. Upon completion of the internal review, SFCM worked to prepare a complete list of individuals requiring notice of this event. This final list of affected individuals was completed on or about January 8, 2021.

**What Information Was Involved?** Our investigation, and that of Blackbaud, determined that the involved Blackbaud systems contained your name and <<impacted data elements>>.

**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 are also offering you access to complimentary credit monitoring and identity protection services for 24 months through CyberScout. These services include fraud consultation and identity theft restoration services. Enrollment instructions can be found in the enclosed *Steps You Can Take to Help Protect Your Information*.

**What You Can Do.** We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and credit reports for suspicious activity. You may also review the information contained in the attached *Steps You Can Take to Help Protect Your Information*. There you will also find more information on the credit monitoring and identity protection services we are making available to you.

**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 800-577-5046 between the hours of 6am to 6pm PST, Monday through Friday except holidays. You can also reach SFCM by writing to 50 Oak St., San Francisco, CA 94102-6011.

We regret any inconvenience or concern this incident may have caused.

Sincerely,

A handwritten signature in black ink, appearing to read 'Kathryn Wittenmyer', with a long, sweeping horizontal line extending to the right.

Kathryn Wittenmyer, VP Finance  
San Francisco Conservatory of Music

## ***STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION***

We are providing you with access to **Single Bureau Credit Monitoring** services at no charge. Services are for 24 months from the date of enrollment. When changes occur to your Experian credit file, notification is sent to you the same day the change or update takes place with the bureau. In addition, we are providing you with proactive fraud assistance to help with any questions you might have. In the event you become a victim of fraud, you will also have access to remediation support from a CyberScout Fraud Investigator. In order for you to receive the monitoring service described above, you must enroll within 90 days from the date of this letter.

**Proactive Fraud Assistance.** For sensitive breaches focused on customer retention, reputation management, or escalation handling, CyberScout provides unlimited access during the service period to a fraud specialist who will work with enrolled notification recipients on a one-on-one basis, answering any questions or concerns that they may have. Proactive Fraud Assistance includes the following features:

- Fraud specialist-assisted placement of fraud alert, protective registration, or geographical equivalent, in situations where it is warranted.
- After placement of a Fraud Alert, a credit report from each of the three (3) credit bureaus is made available to the notification recipient (United States only).
- Assistance with reading and interpreting credit reports for any possible fraud indicators.
- Removal from credit bureau marketing lists while Fraud Alert is active (United States only).
- Answering any questions individuals may have about fraud.
- Provide individuals with the ability to receive electronic education and alerts through email. (Note that these emails may not be specific to the recipient's jurisdiction/location.)

**Identity Theft and Fraud Resolution Services.** Resolution services are provided for enrolled notification recipients who fall victim to an identity theft as a result of the applicable breach incident. ID Theft and Fraud Resolution includes, but is not limited to, the following features:

- Unlimited access during the service period to a personal fraud specialist via a toll-free number.
- Creation of Fraud Victim affidavit or geographical equivalent, where applicable.
- Preparation of all documents needed for credit grantor notification, and fraud information removal purposes.
- All phone calls needed for credit grantor notification, and fraud information removal purposes.
- Notification to any relevant government and private agencies.
- Assistance with filing a law enforcement report.
- Comprehensive case file creation for insurance and law enforcement.
- Assistance with enrollment in applicable Identity Theft Passport Programs in states where it is available and in situations where it is warranted (United States only).
- Assistance with placement of credit file freezes in states where it is available and in situations where it is warranted (United States only); this is limited to online-based credit freeze assistance.
- Customer service support for individuals when enrolling in monitoring products, if applicable.
- Assistance with review of credit reports for possible fraudulent activity.
- Unlimited access to educational fraud information and threat alerts. (Note that these emails may not be specific to the recipient's jurisdiction/location.)

### **How do I enroll for the free services?**

To enroll in Credit Monitoring services at no charge, please navigate to: <https://www.cyberscouthq.com> [REDACTED]

If prompted, please provide the following unique code to gain access to services [REDACTED]

Once registered, you can access Monitoring Services by selecting the "Use Now" link to fully authenticate your identity and activate your services. **Please ensure you take this step to receive your alerts.**

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter.

### **Monitor Accounts**

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:

**Experian**  
PO Box 9554  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com/freeze/center.html](http://www.experian.com/freeze/center.html)

**TransUnion**  
P.O. Box 160  
Woodlyn, PA 19094  
1-888-909-8872  
[www.transunion.com/credit-freeze](http://www.transunion.com/credit-freeze)

**Equifax**  
PO Box 105788  
Atlanta, GA 30348-5788  
1-800-685-1111  
[www.equifax.com/personal/credit-report-services](http://www.equifax.com/personal/credit-report-services)

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 9554  
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)

#### **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](http://www.identitytheft.gov), 1-877-ID-THEFT (1-877-438-4338). 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.

**California Residents:** Visit the California Office of Privacy Protection ([www.oag.ca.gov/privacy](http://www.oag.ca.gov/privacy)) for additional information on protection against identity theft. **Maryland Residents:** Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, [www.oag.state.md.us/Consumer](http://www.oag.state.md.us/Consumer), Telephone: 1-888-743-0023. **New Mexico Residents:** You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting [www.consumerfinance.gov/f/201504\\_cfpb\\_summary\\_your-rights-under-fcra.pdf](http://www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf), or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.



**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; <https://ag.ny.gov/>. **North Carolina Residents:** Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, [www.ncdoj.gov](http://www.ncdoj.gov), Telephone: 1-919-716-6400, 877-566-7226 (toll free within NC). **Oregon Residents:** Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, [www.doj.state.or.us/](http://www.doj.state.or.us/), Telephone: 877-877-9392. **Washington D.C. Residents:** the Office of Attorney General for the District of Columbia can be reached at: 441 4th Street NW, Suite 1100 South, Washington, D.C. 20001; 1-202-442-9828; <https://oag.dc.gov>. **All US Residents:** Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft), 1-877-IDTHEFT (438-4338).