

Holland & Knight

10 St. James Avenue | Boston, MA 02116 | T 617.523.2700 | F 617.523.6850
Holland & Knight LLP | www.hklaw.com

Adam J. Bookbinder
+1 617-305-2038
Adam.Bookbinder@hklaw.com

August 6, 2020

Via E-Mail

Attorney General Wayne Stenehjem
Office of the Attorney General
600 East Boulevard Avenue, Department 125
Bismarck, ND 58505-0040
ndag@nd.gov

Dear Attorney General Stenehjem:

We are writing, pursuant to North Dakota Cent. Code s. 51-30-02, on behalf of our client, New England Conservatory of Music (“NEC”), to notify you of an incident involving the personal information of North Dakota residents.

NEC uses a product offered by Blackbaud, Inc. called *Raiser’s Edge NXT* to manage and track constituent records and data. Blackbaud is one of the world’s largest providers of education administration, fundraising, and financial management software for nonprofit organizations, including higher education institutions.

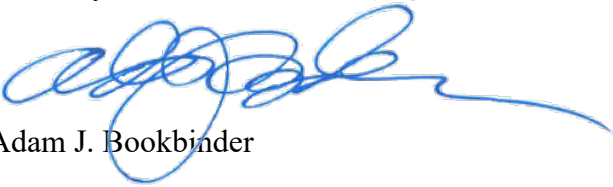
On Thursday, July 16, 2020, NEC received notification that Blackbaud was subject to a ransomware attack in May, 2020. Blackbaud’s notification stated that the cybercriminal removed a copy of certain data from Blackbaud’s servers for the purpose of extorting funds from Blackbaud. NEC determined that this data may have included the personal information of nine North Dakota residents; specifically, their names and dates of birth. We also understand that the impacted data may also have included the individuals’ email addresses and mailing addresses. Blackbaud, however, has indicated that the cybercriminal did not gain access to usernames, passwords, or social security numbers because this data were encrypted. Moreover, neither credit card numbers nor banking information were involved in this incident because the NEC *Raiser’s Edge* database does not collect or store this information.

Based on the nature of the incident, and the research performed by Blackbaud and its outside investigators, Blackbaud has told us there is no reason to believe that any data was accessed by parties other than the cybercriminal responsible for the ransomware attack; was or will be misused; or will be disseminated or otherwise made available publicly. Blackbaud has also told us that it has hired outside experts to continue surveilling for any such activity.

NEC remains in regular contact with Blackbaud regarding the details of this incident, and it is continuing to closely monitor the situation. Pursuant to § 51-30-02, NEC will also be sending notification letters to the North Dakota residents whose personal information was involved in the incident. For your reference, we are enclosing a sample of this notification letter.

Should you have any questions about this matter, please do not hesitate to contact me directly, by phone or email. Thank you for your attention to this matter.

Sincerely,

A handwritten signature in blue ink, appearing to read 'Adam J. Bookbinder', with a long horizontal flourish extending to the right.

Adam J. Bookbinder

Enclosure: Sample notification letter.

SAMPLE NOTIFICATION LETTER

Date
Name
Address
City, State Zip

Dear NEC community member,

On Thursday, July 16, 2020, New England Conservatory received notification from Blackbaud that it discovered it was subject to a ransomware attack in May 2020. Blackbaud is one of the world's largest providers of education administration, fundraising, and financial management software for nonprofits.

At NEC, we use a Blackbaud product called Raiser's Edge NXT to manage and track constituent records and data. The cybercriminal removed data for the purpose of extorting funds from Blackbaud. We determined that your information, specifically name, date of birth, email address, and mailing address may have been accessible. Based on the nature of the incident, the research performed by Blackbaud and its outside investigators, Blackbaud has told us there is no reason to believe that any data went beyond the cybercriminal; was or will be misused; or will be disseminated or otherwise made available publicly. Blackbaud has hired outside experts to continue monitoring for any such activity.

Blackbaud indicated that the cybercriminal **did not** gain access to usernames, passwords, or social security numbers because they were encrypted. And, for your protection, the NEC Raiser's Edge database does not collect or store sensitive information including credit cards numbers or banking information. However, we recommend that all remain observant and report any suspicious activity or suspected identity theft to the proper authorities.

We regret this has taken place and apologize for any concern this may have caused you. We take your privacy very seriously, and we will continue to work diligently to protect your information.

We remain in regular contact with Blackbaud regarding the details of this incident, and we are continuing to monitor their response. Should we receive new or different information, we will provide follow up information.

If you have any immediate concerns or questions, please contact us at privacy@necmusic.edu.

Sincerely,

Kathleen Maddox Kelly
Vice President for Advancement, Engagement & Partnerships
Chief Strategy Officer
New England Conservatory