WILSON ELSER
WILSON ELSER MOSKOWITZ EDELMAN & DICKER LLP

June 16, 2021

Anjali C. Das
312.821.6164 (direct)
Anjali.Das@wilsonelser.com

Via First Class Mail

Attorney General Jane Young
Office of the Attorney General
33 Capitol Street
Concord, NH 03302

Re: Data Security Incident

Dear Attorney General Young:

Wilson Elser Moskowitz Edelman and Dicker LLP ("Wilson Elser") represents Archbishop Mitty High School with respect to a data security incident involving Blackbaud, Inc. (hereinafter, the "Blackbaud Incident") described in more detail below. Archbishop Mitty High School takes the security and privacy of the information in its control seriously, and has taken steps to prevent a similar incident from occurring in the future.

1. Nature of the Security Incident

Blackbaud, Inc. ("Blackbaud") is a cloud computing provider that is used by Archbishop Mitty High School and many other institutions to organize and store information related to members of its community. On September 29, 2020, as your Office may already be aware, Blackbaud notified hundreds of its customers, including Archbishop Mitty High School, that Blackbaud experienced a ransomware event in May 2020 which involved the exposure of data stored by Blackbaud's customers on Blackbaud's platforms. In response to Blackbaud's notification, Archbishop Mitty High School launched an investigation to determine, based on the information provided by Blackbaud, which of its' community were impacted.

2. Number of New Hampshire Residents Affected

During its investigation, Archbishop Mitty High School discovered that the Blackbaud Incident resulted in the unauthorized exposure of information pertaining to one (1) New Hampshire resident. As described below, Archbishop Mitty High School individually notified all potentially affected New Hampshire residents of this incident on June 16, 2021 via First Class Mail.

Specifically, Archbishop Mitty High School notified one (1) New Hampshire resident whose personal information - potentially including their name, social security number, mailing address, telephone number and date of birth - was exposed as a result of the Blackbaud Incident. A sample copy of the incident notification letters mailed to this population of New Hampshire residents is attached as **Exhibit A**.

WILSON ELSER
WILSON ELSER MOSKOWITZ EDELMAN & DICKER LLP

3. Steps Taken

Archbishop Mitty High School mailed incident notification letters addressed to all potentially affected New Hampshire residents on June 16, 2021, via First Class Mail. Additionally, Archbishop Mitty High School is offering notified individuals whose social security numbers were exposed complimentary identity theft and credit monitoring services for a period of twenty-four (24) months. As of this writing, Archbishop Mitty High School has not received any reports of fraud or identity theft related to this matter.

Archbishop Mitty High School remains dedicated to protecting the sensitive information within its control. If you have any questions or need additional information, please do not hesitate to contact me at Anjali.Das@WilsonElser.com or 312-821-6164.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

Anjali C. Das

Enclosure

Return Mail Processing Center
PO 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>>

Dear <<Name 1>>:

We are writing to inform you of a data security incident involving Blackbaud, Inc ("Blackbaud") that has resulted in the exposure of your personal information. Archbishop Mitty High School takes the security of your information very seriously, and we sincerely apologize for any inconvenience this incident may cause. This letter contains information about the incident and resources we are making available to you.

What Happened

Blackbaud is a cloud computing provider that is used by Archbishop Mitty High School and many other educational institutions to organize and store information related to members of our community. In particular, Archbishop Mitty High School utilized Blackbaud's Financial Edge platform for student billing purposes. Certain historical student data stored on the Financial Edge platform included student's Social Security numbers. At the time, Blackbaud assured Archbishop Mitty High School that all social security numbers and dates of birth stored in Financial Edge were encrypted. However, in September 2020, Blackbaud advised Archbishop Mitty High School for the first time that social security numbers, and in some instances, dates of birth, were not in fact encrypted for certain legacy versions of Financial Edge, and that this information was compromised as a result of a cyber-attack on Blackbaud. In response to the September 2020 notice from Blackbaud, Archbishop Mitty High School opened a thorough internal review of the records maintained by our institution via Blackbaud and worked extensively with Blackbaud to determine the scope of this incident and its impact on Archbishop Mitty High School's student and alumni records.

What Information Was Involved

In late September 2020, Blackbaud advised Archbishop Mitty High School that backup files containing personal information of certain former students were exposed to an unauthorized individual(s) following a cyber-attack on Blackbaud. Specifically, these files contained personal information, including your Social Security number. These files may have also included other personal information such as your date of birth, mailing address and telephone number.

According to Blackbaud, and as far as we know, there is no indication that any of the exposed information has been subject to misuse or to further dissemination. Blackbaud has also assured us that they have implemented several changes to protect your data from any subsequent incidents. Again, while we have no evidence that any information related to members of Archbishop Mitty High School's community has been or will be misused, we still encourage you to remain vigilant and immediately report any suspicious activity or suspected misuse of your personal information.

What We Are Doing

Archbishop Mitty High School takes the protection and proper use of your information very seriously. Ensuring the safety of your data is of the utmost importance to us, and we sincerely regret any inconvenience or concern that this may cause. In light of this incident, we are providing you with access to Single Bureau Credit Monitoring services at no charge for twenty-four months (please find instructions below). Further, we continue to monitor the situation and be in close contact with Blackbaud, and we will be sure to keep you apprised of any additional information as it becomes available.

What You Can Do

As mentioned above, Archbishop Mitty High School is providing you with access to Single Bureau Credit Monitoring services at no charge. Services are for twenty-four (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 remediation support from a CyberScout Fraud Investigator.

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: [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 ninety (90) days from the date of this letter.

For More Information

Again, Archbishop Mitty High School takes the protection and proper use of your information very seriously and we sincerely apologize for any concern or inconvenience this letter causes. Should you have any questions or concerns about this matter, please do not hesitate to call 800-536-8304 Monday through Friday between the hours of 6 a.m. and 6 p.m. PST.

Sincerely,

Cathie Whalen
Chief Financial Officer
Archbishop Mitty High School

Additional Important Information

For residents of *Hawaii, Michigan, Missouri, Virginia, Vermont,* and *North Carolina*: It is recommended by state law 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.

For residents of *Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon,* and *West Virginia*:
It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of *Iowa*:
State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *Oregon*:
State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Arizona, Colorado, Maryland, Rhode Island, Illinois, New York, and North Carolina:
You can obtain information from the Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.
Maryland Office of the Attorney General Consumer Protection Division 200, St. Paul Place Baltimore, MD 21202 1-888-743-0023 www.oag.state.md.us
Rhode Island Office of the Attorney General Consumer Protection 150 South Main Street, Providence RI 02903 1-401-274-4400 www.riag.ri.gov
North Carolina Office of the Attorney General Consumer Protection Division, 9001 Mail Service Center Raleigh, NC 27699-9001 1-877-566-7226 www.ncdoj.com
Federal Trade Commission Consumer Response Center, 600 Pennsylvania Ave, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) www.ftc.gov/idtheft
New York Office of Attorney General Consumer Frauds & Protection, The Capitol Albany, NY 12224 1-800-771-7755 https://ag.ny.gov/consumer-frauds/identity-theft
Colorado Office of the Attorney General Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000 www.coag.gov
Arizona Office of the Attorney General Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004 1-602-542-5025
Illinois Office of the Attorney General Consumer Protection Division 100 W Randolph St., Chicago, IL 60601 1-800-243-0618 www.illinoisattorneygeneral.gov

For residents of *Massachusetts*: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft

For residents of all states:
Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf);TransUnion (https://www.transunion.com/fraud-alerts); or Experian (https://www.experian.com/fraud/center.html). 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. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.
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, 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 or a minor under the age of 16, 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. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion (FVAD)**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
https://www.equifax.com/personal/credit-report-services/credit-freeze/	www.experian.com/freeze	freeze.transunion.com
800-525-6285	888-397-3742	800-680-7289

More information can also be obtained by contacting the Federal Trade Commission listed above.