December 31, 2020

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

Via Online Submission

Attorney General Aaron Frey
Office of the Attorney General
6 State House Station
Augusta, ME 04333

Re: Data Security Incident

Dear Attorney General Frey:

Wilson Elser Moskowitz Edelman and Dicker LLP ("Wilson Elser") represents Canterbury School with respect to a data security incident involving Blackbaud, Inc. (hereinafter, the "Blackbaud Incident") described in more detail below. Canterbury 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. Description of the Blackbaud Incident.

Blackbaud, Inc. ("Blackbaud") is a cloud computing provider that is used by Canterbury School and many other institutions to organize and store information related to members of our community.

On July 16, 2020, as your Office may already be aware, Blackbaud first notified hundreds of its customers, including Canterbury 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 July notification, Canterbury School launched an internal investigation to determine, based on the information provided by Blackbaud, which of its' constituents were impacted. Those constituents were notified accordingly on September 9, 2020 (hereinafter, "Canterbury School's September notice"). None of the constituents notified by Canterbury School during Canterbury School's September notice were residents of Maine.

On September 29, 2020, Canterbury School received a second notification letter from Blackbaud (hereinafter, "Blackbaud's September notice"). This letter indicated that it was discovered that additional data maintained by Canterbury School via Blackbaud that was previously believed to be encrypted, was in fact unencrypted and potentially accessible to the threat actor. Following Blackbaud's September notice, Canterbury School re-opened its internal investigation to determine the identities of additional individuals whose personal information was impacted. During this investigation, Canterbury School discovered that two (2) residents of Maine were impacted by the Blackbaud incident. Specifically, the Blackbaud Incident resulted in the

unauthorized exposure of the one (1) Maine resident's personal information, including their bank account numbers and one (1) Maine resident's personal information, including their social security number.

As of this writing, Canterbury School has not received any reports of related identity theft since the date of the incident (May 2020 to present).

2. Number of Maine residents affected.

Two (2) residents of Maine were potentially affected. Incident notification letters addressed to those individuals were mailed on December 31, 2020, via First Class Mail. A sample copy of the Incident notification letters mailed to potentially affected residents of Maine is included with this letter at **Exhibit A**.

3. Steps taken.

Canterbury School has gone to great lengths to identify and notify any individuals who were potentially impacted as result of this Incident with the assistance of a third-party vendor. Additionally, all notified individuals were also offered complimentary identity theft and credit monitoring services for a period of twenty-four (24) months.

4. Contact information.

Canterbury 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

EXHIBIT A

CANTERBURY SCHOOL

EDUCATION • CHARACTER • LEADERSHIP • SERVICE

C/O IDX
P.O. Box 1907
Suwanee, GA 30024

<<First Name>> <<Last Name>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip Code>>

December 31, 2020

Dear <<First Name>> <<Last Name>>:

We are writing to inform you of a data security incident involving Blackbaud, Inc. ("Blackbaud"). Canterbury School ("Canterbury") takes the security of your personal information very seriously, and we sincerely apologize for any inconvenience this incident may cause. This letter contains information about the incident and steps you can take to protect your information.

What happened:
Blackbaud is a cloud computing provider that is used by Canterbury and many other schools and charitable organizations to organize and store information related to members of our community. In July 2020, as you may already be aware, Blackbaud notified hundreds of educational institutions, including Canterbury, that Blackbaud experienced a cybersecurity incident which resulted in the exposure of personal information maintained by educational institutions and charitable organizations on the Blackbaud platform. Canterbury was first notified of this incident by Blackbaud July 16, 2020. Since then, Canterbury has engaged and worked with outside counsel to further investigate the extent of the breach and its impact on our community.

What information was involved:
On September 29, 2020, Canterbury was notified by Blackbaud, and on October 6, 2020, we received the data file from Blackbaud informing that your <<SSN/Bank Account Number>> may also have been exposed as a result of this Incident. At this time, based on the information we have received from Blackbaud, we have no reason to believe that any of your personal information has been misused as a result of this incident. However, for purposes of full disclosure, we feel it is important to inform you that your personal information may have been viewed by unauthorized individuals as a result of this incident.

What are we doing and what you can do:
We have secured the services of CyberScout to provide identity monitoring services at no cost to you, for twenty-four months. While we do not have any evidence of the misuse of your information, we are nonetheless notifying you out of an abundance of caution. Information about the services being provided by CyberScout is included in this letter.

Canterbury is committed to ensuring the security of all personal information in our control, and we are taking steps to prevent a similar event from occurring in the future. As always, we recommend that you continue to join us in remaining vigilant to protect your information.

Other important information:
The protection of your information is a top priority, and we sincerely regret any concern or inconvenience that this matter may cause you. If you have any questions, please do not hesitate to call (833) 754-1802, Monday – Friday, 9:00 am to 9:00 pm, EST.

Sincerely,

George Pappas
Associate Head for Advancement and Strategic Initiatives
Canterbury School

CyberScout Services

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 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.)

Enrollment Instruction - How do I enroll for the free services?

To enroll in Credit Monitoring services at no charge, please navigate to:
https://www.cyberscouthq.com/epiq263?ac=263HQ1173
If prompted, please provide the following unique code to gain access to services: **263HQ1173**

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.

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 *Maryland, Rhode Island, Illinois, New York* and *North Carolina:* You can obtain information from the Maryland and North Carolina 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

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 *District of Columbia*: Office of Consumer Protection, 400 6th Street, NW, Washington, DC 20001 (202) 442-9828 https://oag.dc.gov/consumer-protection

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
www.freeze.equifax.com	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.

CANTERBURY SCHOOL

EDUCATION • CHARACTER • LEADERSHIP • SERVICE

C/O IDX
P.O. Box 1907
Suwanee, GA 30024

<<First Name>> <<Last Name>>
<<Address 1>> <<Address 2>>
<<City>>, <<State>> <<Zip Code>>

December 31, 2020

Dear Family of <<First Name>> <<Last Name>>:

We are writing to inform you of a data security incident involving Blackbaud, Inc. ("Blackbaud"). Canterbury School ("Canterbury") takes the security of your loved one's personal information very seriously, and we sincerely apologize for any inconvenience this incident may cause. This letter contains information about the incident and steps you can take to protect your family loved one's information.

What happened:
Blackbaud is a cloud computing provider that is used by Canterbury and many other schools and charitable organizations to organize and store information related to members of our community. In July 2020, as you may already be aware, Blackbaud notified hundreds of educational institutions, including Canterbury, that Blackbaud experienced a cybersecurity incident which resulted in the exposure of personal information maintained by educational institutions and charitable organizations on the Blackbaud platform. Canterbury was first notified of this incident by Blackbaud July 16, 2020. Since then, Canterbury has engaged and worked with outside counsel to further investigate the extent of the breach and its impact on our community.

What information was involved:
On September 29, 2020, Canterbury was notified by Blackbaud, and on October 6, 2020, we received the data file from Blackbaud informing that your loved one's <<SSN/Bank Account Number>> may also have been exposed as a result of this Incident. At this time, based on the information we have received from Blackbaud, we have no reason to believe that any of your loved one's personal information has been misused as a result of this incident. However, for purposes of full disclosure, we feel it is important to inform you that your loved one's personal information may have been viewed by unauthorized individuals as a result of this incident.

What are we doing and what you can do:
We have secured the services of CyberScout to provide identity monitoring services at no cost to your loved one, for twenty-four months. While we do not have any evidence of the misuse of your loved one's information, we are nonetheless notifying you out of an abundance of caution. Information about the services being provided by CyberScout is included in this letter.

Canterbury is committed to ensuring the security of all personal information in our control, and we are taking steps to prevent a similar event from occurring in the future. As always, we recommend that you continue to join us in remaining vigilant to protect your information.

Other important information:
The protection of your loved one's information is a top priority, and we sincerely regret any concern or inconvenience that this matter may cause you. If you have any questions, please do not hesitate to call (833) 754-1802, Monday – Friday, 9:00 am to 9:00 pm, EST.

Sincerely,

George Pappas
Associate Head for Advancement and Strategic Initiatives
Canterbury School

CyberScout Services

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 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.)

Enrollment Instruction - How do I enroll for the free services?

To enroll in Credit Monitoring services at no charge, please navigate to:
https://www.cyberscouthq.com/epiq263?ac=263HQ1173
If prompted, please provide the following unique code to gain access to services: **263HQ1173**

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.

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 *Maryland, Rhode Island, Illinois, New York* and *North Carolina:* You can obtain information from the Maryland and North Carolina 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

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 *District of Columbia*: Office of Consumer Protection, 400 6th Street, NW, Washington, DC 20001 (202) 442-9828 https://oag.dc.gov/consumer-protection

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
www.freeze.equifax.com	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.