WILSON ELSER
WILSON ELSER MOSKOWITZ EDELMAN & DICKER

December 11, 2020

Richard Reiter
914.872.7728 (direct)
Richard.Reiter@wilsonelser.com

Via First Class Mail

Attorney General Gordon J. MacDonald
Office of the Attorney General
33 Capitol Street
Concord, NH 03302

Re: Data Security Incident

Dear Attorney General MacDonald:

Wilson Elser Moskowitz Edelman and Dicker LLP ("Wilson Elser") represents Delbarton School ("Delbarton") with respect to a data security incident involving Blackbaud, Inc. (hereinafter, the "Blackbaud Incident") described in more detail below. Delbarton 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 Delbarton and many other institutions to organize and store information related to members of its community. On July 16, 2020, as your Office may already be aware, Blackbaud notified hundreds of its customers, including Delbarton, 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, Delbarton launched an investigation to determine, based on the information provided by Blackbaud, which of its' constituents were impacted.

On September 29, 2020, Delbarton received a second notification letter from Blackbaud (hereinafter, "Blackbaud's September notice"). Blackbaud's September notice stated that certain data maintained by Delbarton via Blackbaud that was previously believed by Blackbaud to be encrypted, was in fact unencrypted and accessible to the threat actor responsible for the ransomware event. Following Blackbaud's September notice, Delbarton continued its investigation to determine the identities of additional individuals whose personal information was impacted.

WILSON ELSER

2. Number of New Hampshire Residents Affected

During its investigation, Delbarton discovered that the Blackbaud Incident resulted in the unauthorized exposure of information[1] pertaining to approximately sixty (60) New Hampshire residents. As described below, Delbarton School is individually notifying all potentially affected New Hampshire residents of this incident on December 11, 2020 via First Class Mail.

Specifically, of this population, Delbarton is notifying one (1) New Hampshire resident whose personal information - potentially including their name, social security number, mailing address, email address, telephone number, date of birth, gender, and donor history - was exposed as a result of the Blackbaud Incident. A sample copy of the incident notification letter being mailed to this population of New Hampshire residents is attached as **Exhibit A**.

Additionally, out of an abundance of caution, Delbarton School is notifying an additional fifty-nine (59) residents of New Hampshire whose personal information - including their name, mailing address, email address, telephone number, date of birth, gender, and donor history - was exposed via Blackbaud's platform, but whose social security numbers, according to Blackbaud, *were not exposed*. A sample copy of the Incident notification letters being mailed to residents of New Hampshire on this basis is attached as **Exhibit B**.

3. Steps Taken

Delbarton School will be mailing incident notification letters addressed to all potentially affected New Hampshire residents on December 11, 2020, via First Class Mail. Additionally, Delbarton 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, Delbarton has not received any reports of fraud or identity theft related to this matter.

Delbarton 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 Richard.Reiter@wilsonelser.com or (914) 872-7728.

Very truly yours,

WILSON ELSER MOSKOWITZ EDELMAN AND DICKER LLP

Richard Reiter

Richard Reiter

[1] The exact elements of personal information that were exposed varied per data subject.

WILSON ELSER

EXHIBIT A

DELBARTON SCHOOL
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>>

<<Variable Data 2 >>

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. Delbarton 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 Delbarton School and many other educational institutions to organize and store information related to members of our community. As you may already be aware, in July 2020 Blackbaud notified hundreds of educational institutions, including Delbarton School, that Blackbaud experienced a cybersecurity incident in May 2020 which resulted in the exposure of personal information maintained by educational institutions on the Blackbaud platform.

In response to this incident, Delbarton 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 Delbarton's records. The information that Blackbaud initially provided to Delbarton in July did not indicate that any sensitive personal information belonging to you was affected as a result of this incident. However, in late September 2020, based on further investigation, Blackbaud informed Delbarton School that, in fact, certain elements of your personal information were affected as described below.

What Information Was Involved

Specifically, Blackbaud notified Delbarton School that, in May 2020, Blackbaud discovered and successfully stopped a ransomware attack on its systems. However, in late September 2020, Blackbaud advised that backup files containing certain personal information were exposed to an unauthorized individual(s). Specifically, these files contained personal information including your social security and/or Tax ID number, and may have also included other personal information such as your mailing address, email address, telephone number, date of birth, gender, and donor history.

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 The Delbarton School 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

Delbarton 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. Services are for 24 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, Delbarton School is 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 by March 27, 2021.

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.

For More Information

Again, Delbarton 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 800-783-2145, Monday through Friday, 9am – 9pm ET.

Sincerely,

J. Craig Paris '82,
Assistant Headmaster for Advancement

John Costa,
Director of Technology

AC1133 v.03

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 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
P.O. Box 105788
Atlanta, GA 30348
https://www.equifax.com/personal/credit-report-services/credit-freeze/
800-525-6285

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
www.experian.com/freeze
888-397-3742

TransUnion (FVAD)
P.O. Box 2000
Chester, PA 19022
freeze.transunion.com
800-680-7289

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

WILSON ELSER

EXHIBIT B

DELBARTON SCHOOL
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>>

<<Variable Data 2 >>

Dear <<Name 1>>,

Out of an abundance of caution, we are writing to inform you of a data security incident involving Blackbaud, Inc ("Blackbaud") that may have involved your personal information. Delbarton School takes the security of your information very seriously, and we sincerely apologize for any inconvenience this incident may cause.

What Happened

Blackbaud is a cloud computing provider that is used by Delbarton School and many other educational institutions to organize and store information related to members of our community. As you may already be aware, in July 2020 Blackbaud notified hundreds of educational institutions, including Delbarton School, that Blackbaud experienced a cybersecurity incident in May 2020 which resulted in the exposure of personal information maintained by educational institutions on the Blackbaud platform.

What Information Was Involved

In response to this incident, Delbarton 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 Delbarton's records. Specifically, Blackbaud notified Delbarton School that, in May 2020, Blackbaud discovered and addressed a ransomware attack on its systems. Blackbuad further advised that backup files containing personal information were exposed to an unauthorized individual(s). Specifically, the information contained in these files included personal information such as your name, mailing address, email address, telephone number, date of birth, gender, and donor history.

According to Blackbaud, and as far as we know, there is no indication that any of the compromised information has been subject to misuse or to further dissemination. Further, at this time Delbarton School does not have any evidence that your sensitive personal information, such as your social security number or financial account information, was impacted by this incident.

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 The Delbarton School 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

Delbarton 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. 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

For more information about steps you can take to protect your personal information, please review the enclosed document entitled "Additional Important Information." Among other resources, this page includes instructions on how to place fraud alerts and security freezes on your credit file.

For More Information

Should you have any questions or concerns about this matter, please do not hesitate to call 800-783-2145, Monday through Friday, 9am – 9pm ET.

Sincerely,

J. Craig Paris '82,
Assistant Headmaster for Advancement

John Costa,
Director of Technology

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 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
P.O. Box 105788
Atlanta, GA 30348
https://www.equifax.com/personal/credit-report-services/credit-freeze/
800-525-6285

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
www.experian.com/freeze
888-397-3742

TransUnion (FVAD)
P.O. Box 2000
Chester, PA 19022
freeze.transunion.com
800-680-7289

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