

August 17, 2020

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

VIA EMAIL: securitybreach@atg.wa.gov

Washington State Office of the Attorney General
1125 Washington Street SE
PO Box 40100
Olympia, WA 98504

Re: Data Security Incident

To Whom it May Concern:

Wilson Elser Moskowitz Edelman and Dicker LLP (“Wilson Elser”) represents Gonzaga Preparatory School (“Gonzaga Prep”) with respect to a potential data security incident involving Blackbaud, Inc. (“Blackbaud”), a third-party provider used by Gonzaga Prep to process and store information, as described in more detail below.

1. Nature of the security Incident.

In July 2020, as your Office may already be aware, Blackbaud notified hundreds of educational institutions, including Gonzaga Prep, that Blackbaud experienced a ransomware incident in May 2020 which may have resulted in the exposure of personal information maintained by educational institutions on the Blackbaud platform. Gonzaga Prep was first notified of this incident by Blackbaud on July 16, 2020.

Gonzaga Prep utilizes a Blackbaud platform known as *Raiser’s Edge* to store the following information pertaining to certain residents of Washington State. Based on information Gonzaga Prep received from Blackbaud, Gonzaga Prep believes the following was exposed to and/or obtained by unknown individuals in an unauthorized fashion as a result of this incident: (1) name; (2) address; (3) email address; (4) year of graduation from Gonzaga Prep (if applicable); (5) information related to donations and/or gifts made by an individual to Gonzaga Prep; (6) the name of an individual’s employer; and (7) date of birth. Gonzaga Prep does not use Blackbaud for any payment processing, and does not store the following information on the Blackbaud platform: bank account, credit card information, or social security numbers.

At this time, based on the information Gonzaga Prep received from Blackbaud, Gonzaga Prep has no reason to believe that any personal information of any members of the Gonzaga Prep community has been or will be misused as a result of this incident.

2. Number of Washington State residents affected.

On or about August 7, 2020, Gonzaga Prep finished identifying a population of five thousand (5,000) Washington State residents that were potentially affected by this Incident. Incident notification letters addressed to these individuals were mailed on August 14, 2020, via First Class Mail. Sample copies of the Incident notification letter being mailed to potentially affected residents of Washington are included with this letter as **Exhibit A** and **Exhibit B**.

3. Steps taken.

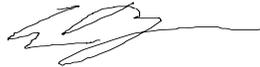
Gonzaga Prep is committed to ensuring the security of all personal information in its control, and is taking steps to prevent a similar event from occurring in the future. Specifically, Gonzaga Prep is re-evaluating its relationship with Blackbaud and the measures that Blackbaud is implementing to secure school data.

4. Contact information.

Gonzaga Prep 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,

p.p.



Richard Reiter

EXHIBIT A



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

Parent or Guardian of
<<Name 1>>
<<Address 1>>
<<City>><<State>><<Zip>>

August 14, 2020

Dear Parent or Guardian of <<Name 1>>:

Out of an abundance of caution, we are writing to inform you of a data security incident involving Blackbaud, Inc. ("Blackbaud"). Gonzaga Preparatory School ("Gonzaga Prep") takes the security of your child's information very seriously, and we sincerely apologize for any inconvenience this incident may cause.

Blackbaud is a cloud computing provider that is used by Gonzaga Prep and many other educational institutions to organize and store information related to our students and members of our community. In July 2020, as you may already be aware, Blackbaud notified hundreds of educational institutions, including Gonzaga Prep, 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. Gonzaga Prep was first notified of this incident by Blackbaud on July 16, 2020.

At this time, based on the information that has been received from Blackbaud, **Gonzaga Prep has no reason to believe that any personal information of any members of the Gonzaga Prep community has been or will be misused as a result of this incident.** However, for purposes of full disclosure, we feel it important to inform you that information we store on Blackbaud was exposed to and/or acquired by unauthorized individuals as a result of this incident.

Specifically, Gonzaga Prep utilizes a Blackbaud platform known as *Raiser's Edge*. Again, while we have no reason to believe any of our students or community members have experienced fraud as a result of this incident, we feel it is important to inform you that Gonzaga Prep uses the *Raiser's Edge* platform to store the following information related to your child which we believe, based on information we received from Blackbaud, was exposed to and/or obtained by individuals in an unauthorized fashion as a result of this incident: (1) your child's name; (2) your child's home address; (3) your child's email address (if applicable) and; (4) and your child's date of birth.

Gonzaga Prep is committed to ensuring the security of all student personal information in our control, and we are taking steps to prevent a similar event from occurring in the future. We are re-evaluating our relationship with Blackbaud and the additional measures that they are implementing to safeguard data. As always, we recommend that you continue to join us in remaining vigilant to protect your child's information.

Again, the protection of your child's information is a top priority, and we sincerely regret any concern or inconvenience that this matter may cause your family. If you have any questions, please do not hesitate to contact our Vice President of Advancement, Corrina Kelsey at (509) 489-6302.

Sincerely,

A handwritten signature in black ink that reads "Michael Dougherty".

Michael Dougherty
President

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](https://assets.equifax.com/assets/personal/Fraud%20Alert%20Request%20Form.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.

EXHIBIT B



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

<<Name 1>>
<<Address 1>>
<<City>><<State>><<Zip>>

August 14, 2020

Dear <<Name 1>>:

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

Blackbaud is a cloud computing provider that is used by Gonzaga Prep and many other educational institutions 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 Gonzaga Prep, 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. Gonzaga was first notified of this incident by Blackbaud on July 16, 2020.

At this time, based on the information Gonzaga Prep has received from Blackbaud, **Gonzaga Prep has no reason to believe that any personal information of any members of the Gonzaga Prep community has been or will be misused as a result of this incident.** However, for purposes of full disclosure, we feel it is important to inform you that we were notified by Blackbaud that information we store on Blackbaud was obtained by unauthorized individuals as a result of this incident.

Specifically, Gonzaga Prep utilizes a Blackbaud platform known as *Raiser's Edge*. Again, while we have no reason to believe any of our community members have experienced fraud as a result of this incident, we feel it is important to inform you that Gonzaga Prep uses the *Raiser's Edge* platform to store the following information related to you which we believe, based on information we received from Blackbaud, was exposed to and/or obtained by unknown individuals in an unauthorized fashion as a result of this incident: (1) your name; (2) your address; (3) your email address; (4) your year of graduation from Gonzaga Prep (if applicable); (5) information related to donations and/or gifts you've made to Gonzaga Prep; (6) the name of your employer; and (7) and your date of birth. Please note that Gonzaga Prep does not use Blackbaud for any payment processing. No bank account, credit card information, or social security numbers are stored in our Blackbaud platform.

Gonzaga Prep 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. We are re-evaluating our relationship with Blackbaud and the measures that they are implementing to secure school data.

Again, the protection of all personal information within our control is a top priority, and we sincerely regret any concern or inconvenience that this matter may cause your family. If you have any questions, please do not hesitate to call our Vice President of Advancement, Corrina Kelsey at (509) 489-6302.

Sincerely,

A handwritten signature in black ink that reads "Michael Dougherty".

Michael Dougherty
President

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.