Michael Best & Friedrich LLP
Attorneys at Law
Adrienne S. Ehrhardt, CIPP/US, CIPM
T 608.283.0131
E asehrhardt@michaelbest.com

August 12, 2020

VIA FEDEX

NH Department of Justice
Gordon J. MacDonald, Attorney General
33 Capitol Street
Concord, NH 03301

RE: Data Breach Notification

Attorney General Gordon J. MacDonald:

Pursuant to N.H. Rev. Stat. §359-C:19, et seq., the Latin School of Chicago, 59 W. North Blvd., Chicago, IL 60610 ("Latin"), through its attorneys Michael Best & Friedrich, LLP, 1 S. Pinckney St., Ste. 700, Madison, WI 53703 ("MBF"), is writing to notify you about a data security incident that occurred at Blackbaud, one of Latin's third party service providers. Latin is a private K-12 school located in Chicago, Illinois. It engages Blackbaud for various cloud services to help manage its philanthropy, alumni engagement, student billing, and internal fund management.

Michael Szczepanek, Chief Financial Officer, mszczepanek@latinschool.org, (312) 582-6102, is Latin's contact, and Adrienne S. Ehrhardt, Partner, asehrhardt@michaelbest.com, (608) 283-0131, from MBF is Latin's legal counsel, assisting with the management of this incident.

We believe that four (4) New Hampshire residents were among this group affected by this breach. Latin is providing these residents with 12 months of free credit monitoring and ID theft restoration through TransUnion.

On July 16, 2020, Blackbaud notified Latin that it suffered a ransomware attack in May 2020, which Blackbaud successfully stopped with the help of independent forensics experts and law enforcement. Unfortunately, the perpetrator was able to copy backups that contained data from Latin and many other schools, colleges, and nonprofits. Blackbaud did, however, pay the requested ransom to ensure the backup file was permanently destroyed.

The personal information that may have been accessed included: names, addresses, telephone numbers, Social Security Numbers, and information relating to the individual's relationship with Latin, such as their philanthropic giving history. Blackbaud generally encrypts sensitive information such as Social Security Number, credit card numbers, or financial account information entered on its systems. However, Latin later discovered that Blackbaud does not encrypt uploaded forms to its systems that may contain such information, and it subsequently determined that some forms containing Social Security Numbers were uploaded to Blackbaud's systems.

Blackbaud has informed Latin that there is no reason to believe that any data went beyond the cybercriminal; was or will be misused; or will be disseminated or otherwise made available publicly.

Blackbaud is working with third party cybersecurity experts and law enforcement to monitor the internet to assist in determining that the information relating to this incident was destroyed. It identified the vulnerability associated with this incident and quickly implemented a security fix. Blackbaud has confirmed through testing by multiple third parties that their fix is able to withstand all currently known cyberattacks. As part of its ongoing efforts to help prevent an incident like this in the future, Blackbaud has implemented additional safety protocols that will help to protect its data. Additionally, Blackbaud is accelerating efforts to enhance access management, backups, encryption, network segmentation, deployment of additional endpoint and network-based platforms.

Attached is a copy of the notification letters that Latin will place in the U.S. Mail Tuesday, August 18, 2020 to the affected individuals. There was no delay in providing individual notification as a result of law enforcement investigation. Please let us know if you have any questions or would like to discuss further.

Sincerely,

MICHAEL BEST & FRIEDRICH LLP

Adrienne S. Ehrhardt

Adrienne S. Ehrhardt

Enclosures

LATIN
SCHOOL of CHICAGO

<<Customer FirstName>> <<Customer LastName>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip Code>>

<<Date>> (Format: Month Day, Year) >>

Notice of Data Breach

Dear <<Customer FirstName>>:

We are writing to inform you about a data security incident that occurred at Blackbaud, one of our third party service providers, that may have involved your personal information. The Latin School of Chicago engages Blackbaud for various cloud services to help manage our philanthropy, alumni engagement, student billing, and internal fund management. Blackbaud recently informed us that it experienced a data breach.

The Latin School of Chicago takes the protection and proper use of your information very seriously. We are therefore contacting you to notify you of the incident and provide you with steps you can take to protect yourself.

What Happened

On July 16, 2020, Blackbaud notified us that it suffered a ransomware attack in May 2020, which it successfully stopped with the help of independent forensics experts and law enforcement. Unfortunately, the perpetrator was able to copy backups that contained data from the Latin School of Chicago and many other schools, colleges, and nonprofits. Blackbaud did, however, pay the requested ransom to ensure the backup file was permanently destroyed.

There was no delay in providing you this notification as a result of law enforcement investigation.

What Information Was Involved

The personal information that may have been accessed included your name, address, telephone number, Social Security Number, and information relating to your relationship with the Latin School of Chicago such as your philanthropic giving history. Blackbaud generally encrypts sensitive information such as Social Security Number, credit card numbers, or financial account information entered on its systems. We later discovered, however, that Blackbaud does not encrypt uploaded forms to its systems that may contain such information, and we determined that a form containing your Social Security Number was uploaded to Blackbaud's systems.

Blackbaud has informed us that there is no reason to believe that any data went beyond the cybercriminal; was or will be misused; or will be disseminated or otherwise made available publicly.

What Our Third-Party Provider is Doing

Blackbaud is working with third party cybersecurity experts and law enforcement to monitor the internet to assist in determining that the information relating to this incident was destroyed. It identified the vulnerability associated with this incident and quickly implemented a security fix. Blackbaud has confirmed through testing by multiple third parties that their fix is able to withstand all currently known cyberattacks. As part of its ongoing cybersecurity efforts to help prevent an incident like this in the future, Blackbaud has implemented additional safety protocols to protect data.

LATIN
SCHOOL of CHICAGO

Additionally, Blackbaud is accelerating efforts to enhance access management, backups, encryption, network segmentation, deployment of additional endpoint and network-based platforms.

What We Are Doing

To help protect you, we have retained TransUnion, a specialist in identity theft prevention to provide you with one year of credit monitoring services, free of charge. To enroll in this service, go to the myTrueIdentity website at www.MyTrueIdentity.com and, in the space referenced as "Enter Activation Code," enter the 12-letter Activation Code provided, or call 1-855-288-5422. We will keep you updated with additional material information if it becomes available, and we will continue to work with Blackbaud to further understand this incident and the steps they are taking to secure our data. Ensuring the safety of our constituents' data is of the utmost importance to us.

What You Can Do

In addition, we are providing you with the enclosed information about Identity Theft Protection which contains helpful information and resources. As a general practice, we recommend that you carefully check your credit reports for accounts you did not open or for inquiries from creditors you did not initiate. If you see anything you do not understand, call the credit agency immediately. You should also regularly review your credit or debit card account statements to determine if there are any discrepancies or unusual activity listed. If you see something you do not recognize, immediately notify your financial institution.

For More Information

We sincerely apologize for this incident and regret any inconvenience it may cause you. We know that some of you may have questions, so please feel free to speak with our representative at the Call Center by dialing 1-866-977-1109 from 9am - 9pm Eastern Time, Monday through Friday. If you have any other questions or concerns regarding this matter, please do not hesitate to contact me at mszczepanek@latinschool.org.

Sincerely,

Michael Szczepanek
Chief Financial Officer
The Latin School of Chicago
59 West North Boulevard
Chicago, IL 60610

Information about Identity Theft Protection

Review Accounts and Credit Reports: It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies. To order your annual 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 from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to:
Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

You should remain vigilant with respect to reviewing your account statements and credit reports, and you should promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding and protection against identity theft: Federal Trade Commission, Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft.

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General: 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.

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from North Carolina Attorney General's Office: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov.

For residents of Rhode Island: You may also obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General: Rhode Island Office of the Attorney General, Consumer Protection Unit, 150 South Main Street, Providence, RI 02903, 401-274-4400, http://www.riag.ri.gov.

Security Freezes and Fraud Alerts:

You have a right to place a security freeze on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. There is no fee for a security freeze. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit.

A security freeze does not apply to a person or entity, or its affiliates, or collection agencies acting on behalf of the person or entity, with which you have an existing account that requests information in your credit report for the purposes of reviewing or collecting the account. Reviewing the account includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements. Please contact the three major credit reporting companies as specified below to find out more information about placing a security freeze on your credit report.

As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on your credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting 7 years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies at the addresses or toll-free numbers listed at the bottom of this page.

Additional Information for Massachusetts Residents: Massachusetts law gives you the right to place a security freeze on your consumer reports at no charge. By law, you have a right to obtain a police report relating to this incident, and if you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. You may request that a freeze be placed on your credit report by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the address below. The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number, date of birth (month, day and year); current address and previous addresses for the past five (5) years; and an incident report or complaint with a law

enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent).

Additional Information for New Mexico Residents: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. Here is a summary of your major rights under the FCRA:

- You have the right to be told if information in your file has been used against you;
- You have the right to receive a copy of your credit report and the right to ask for a credit score;
- You have the right to dispute incomplete or inaccurate information;
- You have the right to dispute inaccurate, incomplete, or unverifiable information;
- You have the right to have outdated negative information removed from your credit file;
- You have the right to limit access to your credit file;
- You have the right to limit "prescreened" offers of credit and insurance you get based on information in your credit report;
- You have the right to seek damages from violators; and
- You have the right to place a "security freeze" on your credit report.

New Mexico Consumers Have the Right to Obtain a Security Freeze or Submit a Declaration of Removal. You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval. The security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place. To remove the freeze or to provide authorization for the temporary release of your credit report, you must contact the consumer reporting agency and may need to provide all of the following:

(1) the unique personal identification number, password or similar device provided by the consumer reporting agency;

(2) proper identification to verify your identity; and

(3) information regarding the third party or parties who are to receive the credit report or the period of time for which the credit report may be released to users of the credit report.

A consumer reporting agency that receives a request from a consumer to lift temporarily a freeze on a credit report shall comply with the request no later than three business days after receiving the request. As of September 1, 2008, a consumer reporting agency shall comply with the request within fifteen minutes of receiving the request by a secure electronic method or by telephone.

A security freeze does not apply in all circumstances, such as where you have an existing account relationship and a copy of your credit report is requested by your existing creditor or its agents for certain types of account review, collection, fraud control or similar activities; for use in setting or adjusting an insurance rate or claim or insurance underwriting; for certain governmental purposes; and for purposes of pre-screening as defined in the federal Fair Credit Reporting Act.

If you are actively seeking a new credit, loan, utility, telephone or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, with enough advance notice before you apply for new credit for the lifting to take effect. You should contact a consumer reporting agency and request it to lift the freeze at least three business days before applying. As of September 1, 2008, if you contact a consumer reporting agency by a secure electronic method or by telephone, the consumer reporting agency should lift the freeze within fifteen minutes. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act.

For more information, including information about additional rights, you can visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf,https://www.consumerfinance.gov/learnmore/, or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed below.

Equifax (www.equifax.com)	Experian (www.experian.com)	TransUnion (www.transunion.com)
General Contact: P.O. Box 740241 Atlanta, GA 30374 800-685-1111 **Fraud Alerts:** P.O. Box 740256 Atlanta, GA 30374 **Credit Freezes:** P.O. Box 105788 Atlanta, GA 30348	**General Contact:** P.O. Box 2002 Allen, TX 75013 888-397-3742 **Fraud Alerts and Security Freezes:** P.O. Box 9554 Allen, TX 75013	**General Contact, Fraud Alerts and Security Freezes:** P.O. Box 2000 Chester, PA 19022 888-909-8872

TransUnion

Activation Code: <<Activation Code>>

Complimentary One-Year *my*TrueIdentity Credit Monitoring Service

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*my*TrueIdentity) for one year provided by TransUnion Interactive, a subsidiary of TransUnion,® one of the three nationwide credit reporting companies.

How to Enroll: You can sign up online or via U.S. mail delivery

- To enroll in this service, go to the *my*TrueIdentity website at **www.MyTrueIdentity.com** and, in the space referenced as "Enter Activation Code," enter the 12-letter Activation Code **<<Insert Unique 12-letter Activation Code>>** and follow the three steps to receive your credit monitoring service online within minutes.
- If you do not have access to the Internet and wish to enroll in a similar offline, paper-based credit monitoring service, via U.S. mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the six-digit telephone passcode **<<Insert static 6-digit Telephone Pass Code>>** and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and **<<Enrollment Deadline>>**. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH COMPLIMENTARY CREDIT MONITORING SERVICE:

- Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score.
- The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more.
- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)