MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Samuel Sica, III
Office: (267) 930-4802
Fax: (267) 930-4771
Email: ssica@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

June 8, 2021

RECEIVED
JUN 14 2021
CONSUMER PROTECTION

VIA U.S. MAIL ONLY

Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Sir or Madam:

We represent the Valencia College Foundation ("Valencia") located in Orlando, Florida with a mailing address of MC: DO-41, PO Box 3028, Orlando, FL 32802-3028, and write to notify your office of an incident that may affect the security of some personal information relating to one (1) New Hampshire resident. By providing this notice, Valencia does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about July 16, 2020, Blackbaud, Inc. ("Blackbaud") notified Valencia, that it experienced a ransomware incident that resulted in encryption of certain Blackbaud systems. Blackbaud reported the incident to law enforcement and worked with forensic investigators to determine the nature and scope of the incident. Following its investigation, Blackbaud notified its customers that an unknown actor may have accessed or acquired certain Blackbaud customer data. Blackbaud reported that the data was accessed or acquired by the threat actor at some point before Blackbaud locked the threat actor out of the environment on May 20, 2020.

While Blackbaud's initial indication was that only name and date of birth were impacted, Valencia continued to work diligently to gather further information from Blackbaud to confirm what information was affected. During September 2020, Blackbaud advised Valencia that additional data types may also have been impacted.

In December 2020, Blackbaud provided added information to allow Valencia to investigate what sensitive data, if any, may have been stored in the additional fields which Blackbaud now identified as potentially accessible.

With assistance from data specialists, Valencia commenced a comprehensive review to identify all personal information potentially accessible. Upon receiving the results of this review, Valencia staff worked diligently to gather further information from its internal records and to confirm last-known addresses in April 2021. Thereafter, Valencia took steps to notify that individual with protected personal information potentially accessible within the impacted Blackbaud database. The information for the New Hampshire resident that could have been subject to unauthorized access includes name, address, and Social Security number.

Notice to New Hampshire Resident

On or about June 8, 2021, Valencia began providing written notice of this incident to affected individuals, which includes one (1) New Hampshire resident. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, Valencia moved quickly to understand the nature of the incident and the results of Blackbaud's investigation, assess the impact on Valencia data, and identify potentially affected individual to provide them with notice of the incident. Valencia is also working review its existing policies and procedures regarding third-party vendors and is working with Blackbaud to evaluate additional measures and safeguards to protect against this type of incident in the future. Valencia is providing access to credit monitoring services for 24 months from CyberScout (through Epiq), to the individual whose Social Security number or tax identification number was potentially affected by this incident, at no cost to this individual.

Additionally, Valencia is providing impacted individual with guidance on how to better protect against identity theft and fraud, by reviewing their account statements, and to monitoring their credit reports for suspicious activity. Valencia is providing the individual with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. Valencia is also notifying other state regulators as required.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4802.

Very truly yours,

Samuel Sica, III of
MULLEN COUGHLIN LLC

SZS/acs

EXHIBIT A

VALENCIA COLLEGE FOUNDATION

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

<<Date>>

<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

Re: Notice of Data Breach

Dear <<Name 1>>:

I appreciate your connection to Valencia, and I hope that you and your family are well.

I write to inform you that Valencia College Foundation was notified by one of its third-party vendors, Blackbaud, Inc. ("Blackbaud"), of a cyber incident that may affect the security of some of your information. Blackbaud is a cloud-computing provider that offers customer-relationship management and financial services tools to non-profit organizations, including Valencia College Foundation. This notice provides information about the Blackbaud incident, our response and resources being made available to you to help protect your information from possible misuse.

What Happened? On July 16, 2020, Blackbaud notified many impacted customers, including Valencia College Foundation, that it experienced a ransomware incident that resulted in encryption of certain Blackbaud systems. Blackbaud reported the incident to law enforcement and worked with forensic investigators to determine the nature and scope of the incident. Following its investigation, Blackbaud notified its customers that an unknown actor may have accessed or acquired certain Blackbaud customer data. Blackbaud reported that the data was accessed or acquired by the threat actor at some point before Blackbaud locked the threat actor out of the environment on May 20, 2020.

While Blackbaud's initial indication was that only name and date of birth were impacted, we continued to work diligently to gather further information from Blackbaud to confirm what information was affected. During September 2020, Blackbaud advised us that additional data types may also have been impacted. In December 2020, Blackbaud provided added information to allow us to investigate what sensitive data, if any, may have been stored in the additional fields which Blackbaud now identified as potentially accessible. With assistance from data specialists, we commenced a comprehensive review to identify all personal information potentially accessible. Upon receiving the results of this review, Valencia Foundation staff worked diligently to gather further information from our internal records and to confirm last-known addresses in April 2021. Thereafter, we took steps to notify those individuals with protected personal information potentially accessible within the impacted Blackbaud database.

What Information Was Involved? You are receiving this notice because our investigation determined that the involved Blackbaud systems contained your <<Breached Elements>>. *Please note that, to date, we have not received confirmation from Blackbaud that your information was specifically viewed or taken by the unknown actor.*

What We Are Doing: The confidentiality, privacy and security of information in our care are among our highest priorities, and we take this Blackbaud incident very seriously. As part of our ongoing commitment to the security of data, we are reviewing our existing policies and procedures regarding third-party vendors, and are working with Blackbaud to evaluate additional measures and safeguards to protect against this type of incident in the future. We are notifying state regulators, as required. Out of an abundance of caution, we are also offering complimentary access to credit monitoring and identity-theft-restoration services for 24 months through CyberScout.

What You Can Do: Please read the enclosed *Steps You Can Take to Help Protect Personal Information*. I encourage you to remain vigilant by reviewing your account statements and free credit reports to ensure accuracy and detect errors. You may also enroll in the complimentary credit-monitoring services. Enrollment instructions are enclosed on the following page.

For More Information: If you have additional questions about the Blackbaud incident, please call our dedicated assistance line at 855-535-1799 between the hours of 9 a.m. and 9 p.m. EST. You may also write to me at Valencia College Foundation, MC: DO-41, PO Box 3028, Orlando, FL 32802-3028.

I am sincerely sorry this incident has occurred. Please take good care.

Sincerely,

Geraldine Gallagher

Geraldine Gallagher
President and Chief Executive Officer

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Enroll in Credit Monitoring and Utilize Identity Restoration Services

As a precautionary measure, we are providing you with; **Single Bureau Monitoring**, access to a Fraud Specialist and remediation support in the event you become a victim of fraud. These services will be available to you at no charge for 24 months and will begin as soon as you complete your registration. 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. To safeguard your privacy and security, you will be asked to verify your identity before monitoring can be activated.

To Register your account and activate your services:

1. Type the following URL into your browser: https://www.cyberscouthq.com/epiq285
2. Click the "Sign Up" button and follow the instructions to create your account.
3. Enter your information and the following Access Code to complete your registration:

   <<Access Code>>

4. Next, click the "Use Now" link on the Monitoring Services tile to verify your identity and activate your monitoring services.

Important - you must register your account and activate your monitoring services within 90 days from the date of this letter, otherwise your ability to access the services will expire.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a 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 seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit 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 credit 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. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th St. NW Washington, D.C. 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are no known Rhode Island residents impacted by this incident.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov/.