MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Julie Siebert-Johnson
Office: (267) 930-4005
Fax: (267) 930-4771
Email: jsjohnson@mullen.law

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

January 4, 2021

VIA U.S. MAIL

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

Re: Notice of the Blackbaud Data Event

Dear Sir or Madam:

We represent Florida Gulf Coast University Foundation, Inc. ("FGCU Foundation") located at 10501 FGCU Blvd., S. Fort Myers, FL 33965, and are writing to notify your office of an incident that may affect the security of some personal information relating to eleven (11) New Hampshire residents. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, FGCU Foundation 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, FGCU Foundation received notification of a cyber incident from one of its third-party vendors, Blackbaud, Inc. ("Blackbaud"). Blackbaud is a cloud computing provider that provides database services tools to organizations and schools, including FGCU Foundation. Blackbaud reported that, in May 2020, it experienced a ransomware incident that resulted in encryption of certain Blackbaud systems. Blackbaud advised that it 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 exfiltrated by the threat actor at some point before Blackbaud locked the threat actor out of the environment on May 20, 2020. While Blackbaud discovered this activity in May 2020, it was not until July 16, 2020 that Blackbaud notified FGCU Foundation that an unknown actor may have accessed or acquired certain Blackbaud customer data.

Upon receiving notice of the cyber incident, FGCU Foundation immediately commenced an investigation to better understand the nature and scope of the incident and any impact on FGCU Foundation data. This investigation included working diligently to gather further information from Blackbaud to understand the scope of the incident and to assess the risk to any FGCU Foundation data stored on impacted systems. On November 20, 2020, FGCU Foundation received further information from Blackbaud about this incident and the scope of the impact to FGCU Foundation data. Thereafter, on or about November 23, 2020, FGCU Foundation received further information from Blackbaud that allowed it to determine the information potentially affected may have contained personal information. On December 5, 2020, after a thorough review process, FGCU Foundation confirmed the population of potentially impacted individuals. FGCU Foundation thereafter worked to confirm the appropriate contact information in order to provide notice to potentially impacted individuals as quickly as possible.

The information that could have been subject to unauthorized access includes information as defined by New Hampshire law including name and financial account information.

Notice to New Hampshire Residents

On or about January 4, 2021, FGCU Foundation provided written notice of this incident to affected individuals, which includes eleven (11) New Hampshire residents. Written notice was provided in substantially the same form as the letter attached hereto as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, FGCU Foundation moved quickly to investigate and respond to the incident, assess the security of FGCU Foundation systems, and notify potentially affected individuals. FGCU Foundation is providing access to credit monitoring services for one (1) year through TransUnion, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, FGCU Foundation is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. FGCU Foundation is also providing individuals 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, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4005.

Very truly yours,

Julie Siebert-Johnson of
MULLEN COUGHLIN LLC

JSJ/mep

EXHIBIT A

Florida Gulf Coast University Foundation
Return Mail Processing Center
P.O. 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>>

Re: Notice of Data <<Variable Heading>>

Dear <<Name 1>>:

Florida Gulf Coast University Foundation, Inc. ("FGCU Foundation") writes to inform you of a recent incident involving one of its third-party vendors, Blackbaud, Inc. ("Blackbaud"), that may affect the privacy of some of your information. While we have no evidence of any actual or attempted misuse of any information as a result of this incident, this notice provides information about the Blackbaud incident, our response and efforts to obtain additional information from Blackbaud, and resources available to you to help protect your information from possible misuse, should you feel it necessary to do so.

What Happened? On Thursday, July 16, 2020, FGCU Foundation received notification from Blackbaud of a cyber incident on its network. Blackbaud is a cloud computing provider that provides database services tools to organizations and schools, including FGCU Foundation. Blackbaud reported that, in May 2020, 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 exfiltrated by the threat actor at some point before Blackbaud locked the threat actor out of the environment on May 20, 2020. Blackbaud discovered this activity in May 2020 and on July 16, 2020 Blackbaud notified FGCU Foundation that an unknown actor may have accessed or acquired certain Blackbaud customer data.

Upon receiving notice of the cyber incident, FGCU Foundation immediately commenced an investigation to better understand the nature and scope of the incident and any impact on FGCU Foundation data. This investigation included working diligently to gather further information from Blackbaud to understand the scope of the incident. On November 20, 2020, FGCU Foundation received further information from Blackbaud about this incident and the scope of the impact to FGCU Foundation data. Additionally, on or about November 23, 2020, FGCU Foundation received further information from Blackbaud that allowed it to determine the information potentially affected may have contained personal information. On December 5, 2020, after a thorough review process, FGCU Foundation confirmed the population of potentially impacted individuals. We thereafter worked to provide notice to potentially impacted individuals as quickly as possible.

What Information is Involved? Our investigation determined that the potentially impacted information included your name and <<Data Elements>>. Please note that, to date, we have not received confirmation from Blackbaud that your specific information was accessed or acquired by the unknown actor.

What Are We Doing? The confidentiality, privacy, and security of information in our care are among our highest priorities, and we take this incident very seriously. FGCU Foundation is continuing to work with Blackbaud to address relevant questions and the next steps that Blackbaud is taking to remediate its data privacy event. We will also be notifying state regulators, as required. Although FGCU Foundation is unaware of any actual or attempted misuse of your information as a result of this incident, as an added precaution FGCU Foundation is offering you access to credit monitoring services through TransUnion for 12 months at no cost to you. Please note that you must complete the enrollment process yourself, as we are not permitted to enroll you in these services on your behalf.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud and to review your account statements and credit reports for suspicious charges. We also encourage you to review the enclosed *Steps You Can Take to Help Protect Your Information*. There you will find general information on what you can do to help protect your personal information.

For More Information. We understand that you may have questions about the Blackbaud incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 800-833-8941 between the hours of 9:00 a.m. and 9:00 p.m. Eastern Time, Monday through Friday. You may also write to Florida Gulf Coast University Foundation at 10501 FGCU Blvd., S., Fort Myers, FL 33965.

We sincerely regret any inconvenience or concern this incident has caused.

Sincerely,

Katherine C. Green
Executive Director
Florida Gulf Coast University Foundation, Inc.

Steps You Can Take to Help Protect Your Information

Enroll in Monitoring Services

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 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 or 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.)

Monitor Accounts

Under U.S. law you are entitled to one (1) free credit report annually from each of the three (3) major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus listed below directly to request a free copy of your credit report.

You have the 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. 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. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 160	P.O. Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior 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.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a one (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 agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19106	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/ fraud-alerts	www.equifax.com/personal/credit-report-services

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); 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 can be reached at: 441 4th St. NW #1100 Washington, D.C. 20001, by phone at (202) 727-3400 and by email at oag@dc.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-410-528-8662, www.oag.state.md.us. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

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 agencies 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 violators. 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 Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; and https://ag.ny.gov/.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6000, www.ncdoj.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

For Rhode Island residents, the Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903; www.riag.ri.gov, 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 approximately 8 Rhode Island residents impacted by this incident.