LEWIS BRISBOIS

LEWIS BRISBOIS BISGAARD & SMITH LLP

Lindsay B. Nickle
2100 Ross Avenue, Suite 2000
Dallas, Texas 75201
Lindsay.Nickle@lewisbrisbois.com
Direct: 214.722.7141

May 26, 2022

VIA ELECTRONIC SUBMISSION
Attorney General Brian E. Frosh
Office of the Attorney General
Attn: Security Incident Notification
200 St. Paul Place
Baltimore, MD 21202
Email: Idtheft@oag.state.md.us

Re: **Notification of Data Security Incident**

Dear Attorney General Frosh:

Lewis Brisbois Bisgaard & Smith LLP represents Martin University ("Martin"), a private college located in Indianapolis, Indiana in connection with a recent data security incident described in greater detail below.

1. Nature of the Security Incident

On January 3, 2022, Martin discovered unusual activity in their computer network. Upon discovery, Martin took immediate steps to secure its systems. On January 5, 2022, Martin learned that their systems had been encrypted as a result of a ransomware attack. Martin retained outside cybersecurity experts to conduct an investigation to determine the source and scope of the incident as well as negotiate with the threat actor group responsible, AvosLocker. The forensic investigation revealed that AvosLocker gained access to Martin's network and encrypted the servers. Martin reached a resolution and made a ransom payment to AvosLocker on January 12, 2022. Upon payment, Martin took steps to recover and restore their environment.

Communications with the threat actor and the forensic investigation demonstrated that the threat actor did access and exfiltrate data from the Martin University environment. On February 7, 2022, Martin discovered indicators that the exfiltrated data may contain personal information. However, because the attack resulted in extensive corruption of data within the Martin University network, it was difficult to determine the specific information that had been impacted and the individuals the information pertained to. Martin's retained experts took extensive steps to recover and restore the corrupted data. Those steps were partially successful, but Martin was unable to recover the precise data that was exfiltrated from the environment. After Martin exhausted all options for restoration and recovery of the data, based upon the evidentiary indicators of where in the environment the data was exfiltrated from, Martin made the decision to notify current and former students from January 2017

through January of 2022, and thereafter, Martin worked to identify address information for those current and former students and prepared notification materials. However, because recovery of the impacted data was not possible, in order to reach additional, potentially impacted individuals, Martin also issued a state-wide press release in Indiana to notify individuals whose identities and address information were not recoverable following the attack.

2. Type of Information and Number of Maryland Residents Involved

A total of 1 resident of Maryland was sent a notification letter about this incident. The information involved may include individual's name and federal student financial aid information. The notification letter was mailed via USPS First Class Mail on May 26, 2022. A sample copy of that letter is included with this notice. Additionally, the state-wide press release in Indiana was also released on May 26, 2022. A copy of the press release is attached with this notice.

3. Measures Taken to Address the Incident

Upon learning of this incident, Martin took steps to secure its environment. Additionally, Martin engaged a computer forensics firm to conduct an investigation into the incident and communicate with the threat actor. Finally, Martin has notified potentially impacted individuals and provided them with information about steps they can take to help protect their personal information as well as offering complimentary identity protection services, 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services.

4. Contact Information

Martin is dedicated to protecting the sensitive information within its control. If you have any questions or need additional information regarding this incident, please do not hesitate to contact Lindsay Nickle at Lindsay.Nickle@lewisbrisbois.com.

Sincerely,

Lindsay Nickle of
LEWIS BRISBOIS BISGAARD & SMITH LLP

MARTIN
UNIVERSITY

10300 SW Greenburg Rd.
Suite 570
Portland, OR 97223

To Enroll, Please Call:
1-800-939-4170
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code:
<<XXXXXXXX>>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

May 26, 2022

Re: Notice of Data Security Incident

Dear <<First Name>> <<Last Name>>,

We are writing to inform you about a recent incident experienced by Martin University ("Martin") that may have impacted your personal information. Martin, like many other colleges and universities across the nation, experienced a recent ransomware attack. The university learned of the suspicious activity on January 3, 2022. We immediately hired security experts and a computer forensic investigator to analyze the system, ensure its safety, and determine whether the incident impacted anyone's personal information.

At no time were courses and instruction disrupted, and students were able to continue attending classes virtually. Although the incident prevented access to student services and financial systems, along with some financial aid transactions, Martin's cyber security consultants and Information Technology team worked diligently to regain access to the impacted systems.

Our investigation revealed that this network incident may have impacted the personal information of some current, former, and prospective students.

The university learned that the information that may have been involved includes your name, <<variable text>>. Although there has been no evidence to suggest that any student information was viewed or misused by the attackers, we wanted you to be aware of the results of our thorough investigation.

The university is sending this letter to those potentially affected; to tell you about the incident; offer you credit monitoring and identify remediation services; and provide you with information, resources, and steps you can take to protect your personal data.

We take the privacy and security of all individuals' personal information very seriously. When we became aware of suspicious activity on our computer network, we immediately took steps to investigate the activity and began a process to enhance the security of our system. In addition, we have implemented additional measures to enhance the security of our computer environment in an effort to minimize the likelihood of a similar event occurring in the future. Our efforts allowed us to rebound faster than expected, although the recovery process is still ongoing. Our internal team and outside cybersecurity experts have been hard at work and will continue until all recovery efforts have been completed.

We are providing you with information regarding steps that you can take to help protect your information. As an added precaution, Martin is offering you complimentary identity protection services through IDX, a data breach and recovery services expert. Your services include <<12 or 24>> months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, IDX will help you resolve

issues if your identity is compromised. Please note the deadline for you to enroll in the services being offered to you is August 26, 2022.

Although Martin is not aware of the misuse of any information potentially impacted in connection with this incident, we encourage you to review the recommendations on the following page to help protect your information. We also encourage you to contact IDX with any questions and to enroll in the free identity protection services being offered to you by calling 1-800-939-4170 or going to https://app.idx.us/account-creation/protect and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 a.m. to 9 p.m. Eastern Time. IDX representatives are fully versed on the incident and can answer questions or concerns you may have regarding protection of your information.

If you have any questions regarding this incident or would like assistance enrolling in the services offered, please call 1-800-939-4170, Monday through Friday from 9 a.m. to 9 p.m. Eastern Time. You will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

The security of our student information is a top priority for Martin, and we are committed to safeguarding your data. We sincerely apologize for any inconvenience that this matter may cause.

Sincerely,

Dr. Sean Huddleston
President
Martin University

Additional Steps You Can Take to Protect Your Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Request a Copy of Your Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting https://www.annualcreditreport.com, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax
P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Place a Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at https://www.annualcreditreport.com.

Put a Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you, including your full name, Social Security Number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission (FTC)
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General
Bureau of Internet and Technology Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
http://www.riag.ri.gov
1-401-274-4400

Washington D.C. Attorney General
441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA and your rights pursuant to the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.

MARTIN UNIVERSITY ANNOUNCES DATA SECURITY INCIDENT

INDIANAPOLIS – Martin University today announced that it, like many other colleges and universities across the nation, experienced a recent ransomware attack. The university learned of the suspicious activity on January 3, 2022. It immediately hired security experts and a computer forensic investigator to analyze the system, ensure its safety, and determine whether the incident impacted anyone's personal information.

At no time were courses and instruction disrupted and students were able to continue attending classes virtually. Although the incident prevented access to student services, financial systems, along with some financial aid transactions, Martin's cyber security consultants and Information Technology team worked diligently to regain access to the impacted systems.

"Our investigation revealed that this network incident may have impacted the personal information of some current, former, and prospective students," said Dr. Sean Huddleston, President. "The university learned that the attackers may have gained access to some of its student's personal information, although there has been no evidence to suggest that any student information was viewed or misused by the attackers."

The university has attempted to contact those affected; tell them about the incident; offer them credit monitoring and identify remediation services; and provide them with information, resources, and steps they can take to protect their personal data.

"We take the privacy and security of all individuals' personal information very seriously," said Huddleston, "When we became aware of suspicious activity on our computer network, we immediately took steps to investigate the activity and began a process to enhance the security of our system. Our efforts allowed us to rebound faster than expected, although the recovery process is still ongoing. Our internal team and outside cybersecurity experts have been hard at work and will continue until all recovery efforts have been completed."

On May 26th, 2022, notification letters were sent to the potentially affected individuals Martin has been able to identify. Current or former students of Martin or prospective students between January 2017 and January 2022 who have not been notified about this incident should call 1-800-939-4170 Monday through Friday from 8am – 8pm Central Time for further information or to enroll in a complimentary identity protection service through IDX to those individuals whose protected information was potentially affected in connection with this incident.

Due to the impact of the incident on the Martin computer environment, some potentially impacted individuals have not been identified, and as a result Martin has not been able to send letters to those potentially impacted individuals. If you are a current or former student of Martin, or if you were a prospective student of Martin between January of 2017 and January of 2022 and you did not receive a notification letter about this incident, please call 1-800-939-4170 for further information or to enroll in complimentary identity monitoring services.

“Our students are a top priority at Martin, and we are committed to safeguarding their information. We value transparency with students and stakeholders amid this untimely incident,” said Huddleston.

For further details regarding this incident, visit www Martin.edu.

Founded in 1977, Martin University is Indiana’s only Predominantly Black Institution of higher education. It is steeped in a history of service and open to a diverse population of students. Its mission is to elevate the landscape while providing transformative opportunities, inclusive support, and service to our communities.