LEWIS BRISBOIS

LEWIS BRISBOIS BISGAARD & SMITH LLP

Alyssa R. Watzman
1700 Lincoln Street, Suite 4000
Denver, CO 80203
Alyssa.Watzman@lewisbrisbois.com
Direct: 720.292.2052

June 1, 2020

VIA Email (DOJ-CPB@doj.nh.gov)
Attorney General Gordon MacDonald
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301

Re: Notification of Potential Data Security Incident

Dear Attorney General MacDonald:

We represent Paul Quinn College ("PQC") in connection with a recent data security incident described in greater detail below. PQC has taken steps to notify the potentially impacted individuals and enhance the security of its systems in an effort to prevent similar incidents from occurring in the future.

1. Nature of the security incident.

On August 16, 2019, PQC learned that certain PQC employee email accounts had been accessed without authorization. In immediate response, PQC took steps to secure the impacted email accounts and to further secure its email system, and it began an extensive and detailed analysis of the email accounts to determine if they contained any personal information that may have been affected by the incident. The analysis was completed on February 19, 2020, and it revealed that some personal information was contained in the email accounts involved in the incident. The information potentially involved in the incident includes the name and Social Security number of a single resident of New Hampshire.

After the analysis was complete, PQC worked diligently to identify current address information for the potentially affected individuals in order to effectuate notification and took steps to complete notification quickly as possible in light of significant challenges arising from responding to the COVID-19 situation.

PQC has no evidence to suggest that any personal information involved in this incident has been misused. Nonetheless, out of an abundance of caution, potentially affected individuals for whom address information was identified were notified about the incident on June 1, 2020 and offered complimentary identity monitoring services through ID Experts.

2. Number of New Hampshire residents affected.

PQC notified 1 New Hampshire resident regarding this data security incident. Notification letters were mailed via first class U.S. mail on June 1, 2020. A sample copy of the notification letter is included with this letter.

3. Steps taken relating to the incident.

PQC has taken steps in response to this incident to further strengthen the security of its email system in an effort to prevent similar incidents from occurring in the future. In addition, PQC has notified the affected resident and offered the individual twelve months of credit monitoring and identity protection services at no charge to the individual.

4. Contact information.

PQC remains dedicated to protecting the personal information in its control and has taken steps to enhance the security of its email system and reduce the risk of a similar incident occurring in the future. If you have any questions or need additional information, please do not hesitate to contact me at (720) 292-2052 or alyssa.watzman@lewisbrisbois.com.

Sincerely,

Alyssa Watzman

LEWIS BRISBOIS BISGAARD & SMITH LLP

Enclosure: Sample Patient Notification Letter

C/O ID Experts
PO Box 4219
Everett WA 98204

ENDORSE

NAME
ADDRESS1
ADDRESS2
CSZ
COUNTRY

BREAK

SEQ
CODE 2D
Ver 1

To Enroll, Please Call:
1-833-579-1102
Or Visit:
https://ide.myidcare.com/pqc
Enrollment Code: <<XXXXXXXX>>

June 1, 2020

Subject: Notice of Data Security Incident

Dear <<First Name>> <<Last Name>>:

I am writing to inform you of a data security incident experienced by Paul Quinn College ("PQC") that may have involved your personal information. PQC sincerely regrets any concern that this incident may cause you. This letter is intended to provide you with information about the incident as well as to inform you of steps that can be taken to help protect your information.

What Happened? On August 16, 2019, we learned that certain PQC employee email accounts had been accessed without authorization. In immediate response, we took steps to secure the impacted email accounts and to further secure our email system, and we began an extensive and detailed analysis of the email accounts to determine if they contained any personal information that may have been affected by the incident. The analysis was completed on February 19, 2020, and it revealed that some of your information was contained in the affected email accounts. After the analysis was complete, we worked diligently to identify up-to-date address information in order to effectuate notification and took steps to notify you of this incident as quickly as possible in light of significant challenges arising from responding to the COVID-19 situation.

We have no evidence to suggest that your personal information has been misused. Nonetheless, out of an abundance of caution, we are writing to inform you about the incident and to share with you steps you can take to help protect your personal information.

What Information Was Involved? The following information may have been involved in the incident: your name and <<Variable Data>>.

What Are We Doing? As soon as we discovered this incident, we took the steps described above with the assistance of independent cybersecurity experts engaged to assist. Additionally, although we are not aware of any misuse of your information, we have engaged ID Experts® - a leading data security incident and recovery services vendor - to provide you with complimentary MyIDCare™ services for twelve (12) months to assist you. These services include Credit and CyberScan Dark Web Monitoring, a $1,000,000 identity theft insurance reimbursement policy, and fully managed identity recovery services. With this protection, MyIDCare™ will help you resolve issues arising from an identity compromise.

What You Can Do: While we are not aware of any misuse of information involved in this incident, we encourage you to follow the recommendations included on the following page. We also encourage you to enroll in the complimentary MyIDCare™ services being offered to you as a precautionary measure by going to https://ide.myidcare.com/pqc or by calling 1-833-579-1102 and using the Enrollment Code provided above. MyIDCare™ experts are available Monday through Friday from 8 am to 8 pm Central Time. Please note the deadline to enroll is August 31, 2020.

For More Information: Further information about how to protect your personal information appears on the following page. If you have questions please call 1-833-579-1102 from 8 am to 8 pm Central Time, Monday through Friday.

Thank you for your patience through this incident. Please accept our sincere apologies and know that PQC deeply regrets any worry or inconvenience that this may cause you.

Sincerely,

Bruce Brinson
Chief Financial Officer
Paul Quinn College

STEPS YOU CAN TAKE TO FURTHER 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).

Copy of 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 http://www.annualcreditreport.com/, calling toll-free 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:

TransUnion	**Experian**	**Equifax**	**Free Annual Report**
P.O. Box 1000	P.O. Box 2002	P.O. Box 740241	P.O. Box 105281
Chester, PA 19016	Allen, TX 75013	Atlanta, GA 30374	Atlanta, GA 30348
1-800-916-8800	1-888-397-3742	1-866-349-5191	1-877-322-8228
www.transunion.com	www.experian.com	www.equifax.com	annualcreditreport.com

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 90 days. 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 http://www.annualcreditreport.com.

Security Freeze: Under U.S. law, 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	**Maryland Attorney General**	**North Carolina Attorney General**	**Rhode Island Attorney General**
600 Pennsylvania Ave	200 St. Paul Place	9001 Mail Service Center	150 South Main
Washington DC 20580	Baltimore, MD 21202	Raleigh, NC 27699	Providence, RI
consumer.ftc.gov	oag.state.md.us	ncdoj.gov	02903
www.ftc.gov/idtheft	1-888-743-0023	1-877-566-7226	www.riag.ri.gov
1-877-438-4338			401-274-4400

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 http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

Protecting personal information of a Minor: Contact the three national credit reporting agencies to request a search for a credit report associated with a minor's Social Security number. If a report exists, request a copy and immediately report fraudulent accounts to the credit reporting agency. You can also report any misuse of minor's information to the FTC at https://www.identitytheft.gov/. For more information visit: https://www.consumer.ftc.gov/articles/0040-child-identity-theft.

SEQ
CODE 2D