



Laura Funk
2100 Ross Avenue, Suite 2000
Dallas, Texas 75201
Laura.Funk@lewisbrisbois.com
Direct: 972.942.5696

August 19, 2022

File No. 49905.138

VIA ELECTRONIC SUBMISSION

Attorney General Brian E. Frosh
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD. 21202
Email: IDtheft@oag.state.md.us

Re: Notice of Data Security Incident

Dear Attorney General Frosh:

Lewis Brisbois Bisgaard & Smith LLP (“Lewis Brisbois”) represents Pearl River Community College (“PRCC”) in connection with a recent data security incident, described in greater detail below. PRCC is a junior college located in Poplarville, Mississippi. The purpose of this letter is to notify you of the incident in accordance with Maryland’s data breach notification statute. (Md. Code Ann. Comm. Law §§ 14-3501-3508).

1. Nature of the Security Incident

On April 30, 2022, PRCC discovered that it had experienced an incident disrupting access to systems within its network. In response, PRCC took immediate steps to secure its systems and promptly launched an investigation. In so doing, PRCC engaged independent digital forensics and incident response experts to determine what happened and to identify any information that may have been accessed or acquired without authorization as a result. On July 21, 2022, PRCC learned that personal information belonging to certain individuals may have been impacted in connection with the incident. PRCC then took steps to identify current mailing addresses in order to effectuate notification to potentially impacted individuals.

The information that may have been accessible by the malicious actor(s) responsible for this incident included first and last name(s) and Social Security number(s).

2. Number of Maryland Resident(s) Affected

PRCC notified seven (7) Maryland residents of this incident via First-Class U.S. Mail on August 19, 2022. A sample copy of the notification letter is included with this correspondence.

3. Steps Taken Relating to the Incident

As soon as PRCC discovered this incident, PRCC took steps to secure its systems and launched an investigation to determine what happened and whether personal information had been accessed or acquired without authorization. PRCC has also implemented additional safeguards to help ensure the security of its systems and to reduce the risk of a similar incident occurring in the future. Additionally, PRCC reported the incident to the Federal Bureau of Investigation and will cooperate with law enforcement activity.

PRCC has also established a toll-free call center through IDX, a leader in risk mitigation and response, to answer any questions about the incident and address related concerns. While PRCC is not aware of the misuse of any information as a result of this incident, out of an abundance of caution, PRCC is also providing complimentary identity protection services to notified individuals for a period of 12 months. These services include credit and CyberScan monitoring, identity restoration, and a \$1 million identity theft insurance policy.

4. Contact Information

PRCC remains dedicated to protecting the personal information in its control. If you have any questions or need additional information, please do not hesitate to contact me at 972.942.5696 or Laura.Funk@lewisbrisbois.com.

Best regards,



Laura K. Funk
LEWIS BRISBOIS BISGAARD & SMITH LLP

Enclosure: Sample Consumer Notification Letter



Return Mail to IDX
P.O. Box 989728
West Sacramento, CA 95798-9728

To Enroll, Please Call:
1-833-764-2926
Or Visit:
<https://response.idx.us/prcc>
Enrollment Code: <<ENROLLMENT>>

<<FIRST NAME>> <<LAST NAME>>
<<ADDRESS1>>
<<ADDRESS2>>
<<CITY>>, <<STATE>> <<ZIP>>
<<Country>>

August 19, 2022

Re: Notice of Data <<Variable Text 1: Breach/Security Incident>>

Dear <<FIRST NAME>> <<LAST NAME>>,

We are writing to inform you of a data security incident experienced by Pearl River Community College ("PRCC") that may have affected your personal information. PRCC takes the privacy and security of all student and personal information within its possession very seriously. Please read this letter carefully as it contains information regarding the incident and steps you can take to help protect your personal information.

What Happened. On April 30, 2022, PRCC discovered that it had experienced an incident disrupting access to systems within its network. In response, PRCC took immediate steps to secure its systems and promptly launched an investigation. In doing so, we engaged independent digital forensics and incident response experts to determine what happened and to identify any information that may have been accessed or acquired without authorization as a result.

On July 21, 2022, PRCC learned that your personal information may have been impacted in connection with the incident, which is the basis for this notification. Please note that we have no evidence of the misuse or attempted misuse of any potentially impacted information.

What Information Was Involved. The information involved included your name and Social Security number.

What Are We Doing. As soon as PRCC discovered the incident, we took the steps described above. In addition, PRCC implemented measures to enhance the security of its digital environment in an effort to minimize the risk of a similar incident occurring in the future. We also reported this incident to the Federal Bureau of Investigation and will cooperate with law enforcement efforts.

Although PRCC has no evidence of the misuse of any potentially impacted information, PRCC is providing you information about steps you can take to help protect your personal information and is offering you complimentary identity protection services through IDX – a data breach and recovery services expert. These services include: <<12/24>> months of credit¹ and CyberScan monitoring, a \$1 million identity fraud loss reimbursement policy, and fully managed identity theft recovery services. Please note that the deadline to enroll is November 19, 2022.

¹ To receive credit monitoring services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

What You Can Do. You can follow the recommendations included with this letter to help protect your personal information. PRCC also encourages you to review your credit report for unusual activity. If you see anything that you do not understand or that looks suspicious, you should contact the consumer reporting agencies for assistance using the contact information included with this letter.

For More Information: Further information about how to protect your personal information appears on the following page. If you have any questions or need assistance, please call IDX at 1-833-764-2926 from 08:00 A.M. to 08:00 P.M. Central Time, Monday through Friday (excluding holidays). IDX call center representatives are fully versed on this incident and can answer any question that you may have.

The security of your information is a top priority at Pearl River Community College, and we are committed to safeguarding your data. Please accept our sincere apologies and know that we take this matter seriously and deeply regret any worry or inconvenience that this may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read 'Adam Breerwood', with a stylized flourish at the end.

Dr. Adam Breerwood
President, Pearl River Community College

Enclosure

Additional Steps You Can Take to Protect Your Personal 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).

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

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 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	Experian	TransUnion	Free Annual Report
P.O. Box 105851	P.O. Box 9532	P.O. Box 1000	P.O. Box 105281
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-800-525-6285	1-888-397-3742	1-800-916-8800	1-877-322-8228
www.equifax.com	www.experian.com	www.transunion.com	www.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 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 <http://www.annualcreditreport.com>.

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. Residents of Maryland, North Carolina, and Rhode Island can obtain more information from their Attorney General's Office using the contact information below.

Iowa: You are advised to report any suspected identity theft to law enforcement or to the Office of the Attorney General of Iowa, 1305 E Walnut St, Des Moines, IA 50319, 1- 888-373-5044, <https://www.iowaattorneygeneral.gov/>.

Maine: Maine Attorney General can be reached at: 6 State House Station Augusta, ME 04333; 207-626-8800; <https://www.maine.gov/ag/>.

Maryland: Maryland Attorney General can be reached at: 200 St. Paul Place Baltimore, MD 21202; 1-888-743-0023; oag@state.md.us or IDTheft@oag.state.md.us

North Carolina: North Carolina Attorney General's Office, Consumer Protection Division, can be reached at: 9001 Mail Service Center Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; www.ncdoj.gov

Oregon: You may also contact the Oregon Office of the Attorney General: Oregon Department of Justice, 1162 Court St. NE, Salem, OR 97301-4096, 1-877-877-9392, help@oregonconsumer.gov, www.doj.state.or.us.

New York: New York Attorney General can be reached at: Bureau of Internet and Technology Resources, 28 Liberty Street, New York, NY 10005, 1-212-416-8433, <https://ag.ny.gov/>.

Rhode Island: Rhode Island Attorney General can be reached at: 150 South Main Street Providence, RI 02903, <http://www.riag.ri.gov>.

Vermont: Vermont Attorney General's Office can be reached at: 109 State Street, Montpelier, VT 05609; Phone (802) 828-3171; Email: ago.info@vermont.gov.

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

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