SAUL EWING
ARNSTEIN
& LEHR LLP

David T. Shafer
Phone: (410) 332-8742
Fax: (410) 332-8176
David.Shafer@saul.com
www.saul.com

November 8, 2017

[Sent via Federal Express]

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

Dear Attorney General MacDonald:

This firm represents the Baylor College of Medicine ("BCM"), a health sciences university located in Houston, Texas. In late October 2016, BCM discovered that a database containing information about applicants to the school may have been compromised, resulting in the possible exposure of applicants' personal information. The personal information that may have been exposed and accessed included the first name, middle initial, last name and Social Security number of individuals who submitted applications to BCM. As a result of the incident, the information of approximately 1 New Hampshire resident was likely exposed to unauthorized access. At that time, BCM took immediate action to correct the vulnerability and notify the affected individuals and the Office of the Attorney General of New Hampshire.

Recently, in October of 2017, BCM was alerted that the information contained in the database previously accessed in 2016 had been made available by an unknown third-party on a publicly-accessible website. BCM has since engaged the services of an outside consultant to perform an independent technical analysis and is not aware of any new unauthorized access to or breach of BCM systems since the October 2016 incident. Out of an abundance of caution, BCM will be notifying the affected individuals on November 8, 2017 by U.S. mail and offering certain credit monitoring services; a copy of the sample notification letter is attached.

Contact information for BCM is as follows:

Baylor College of Medicine
One Baylor Plaza
Houston, TX 77030
Primary Contact: Robert F. Corrigan, Jr.
Telephone: 713-798-6392

If you should have any questions or need further information, please don't hesitate to contact us.

Sincerely,

David T. Shafer

Baylor College of Medicine

RANDY LANGENDERFER
Vice President,
Chief Compliance
and Audit Officer

ONE BAYLOR PLAZA
MS: BCM625
HOUSTON, TEXAS 77030

<<MemberFirstName>> <<MemberLastName>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip Code>>

<<Date>> (Format: Month Day, Year)

Notice of Possible Data Breach

Dear <<MemberFirstName>> <<MemberLastName>>,

We are writing to tell you about a data security incident that may have exposed some of your personal information. We take the protection and proper use of your information very seriously. For this reason, we are contacting you directly to explain the circumstances of the incident.

What happened?

In late October of 2016, Baylor College of Medicine discovered that a database containing information about applicants to the school may have been compromised, and immediately began investigating. We confirmed that there was a vulnerability in the database that could have resulted in exposure of personal information, and we took immediate action to correct that vulnerability.

Recently, in October of 2017, Baylor College of Medicine was alerted that the information contained in the database previously accessed in 2016 had been made available by an unknown third-party on a publicly-accessible website. We engaged the services of an outside consultant who confirmed that there was not only exposure of your personal information, but unauthorized access to it as well. We are not aware of any new unauthorized access to or breach of our systems that has occurred since October of 2016; however, out of an abundance of caution, we wanted to let you know about the exposure of your information and extend to you certain services as detailed below. <<ClientDef1(Rhode Island Population: Baylor College of Medicine estimates that personal information of approximately 1 individual in Rhode Island may have been impacted.)>>

What information was involved?

The information involved included the <<ClientDef2(SSN Population: first name, middle initial, last name, and Social Security number / No SSN Population: first name, middle initial, and last name)>> of certain individuals, including you, who submitted applications to Baylor College of Medicine. There was exposure of and unauthorized access to this information.

What we are doing.

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Web Watcher, Public Persona, Quick Cash Scan, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit **my.idmonitoringservice.com** to enroll and take advantage of your identity monitoring services.

You have until **March 1, 2018** to activate your identity monitoring services.

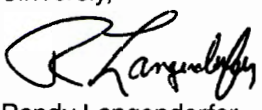
Membership Number: **<<Member ID>>**

To receive credit services by mail instead of online, please call 1-833-210-8119. Additional information describing those services is included with this letter.

For more information.

If you have questions, please call 1-833-210-8119, Monday through Friday from 8:00 a.m. to 5:00 p.m. Central Time. In addition, the United States Department of Education maintains a website describing steps you may take if your information may have been subject to unauthorized access. The URL for that website is: https://www2.ed.gov/about/offices/list/oig/misused/idtheft.html.

Sincerely,



Randy Langenderfer
Vice President, Chief Compliance and Audit Officer

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies is:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 19022, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual free credit report please visit **www.annualcreditreport.com** or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alert. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit.

Security Freeze. You have the ability to place a security freeze on your credit report.

A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. The credit reporting agencies may charge a fee to place a freeze, temporarily lift it or permanently remove it. The fee is waived if you are a victim of identity theft and have submitted a valid investigative or law enforcement report or complaint relating to the identity theft incident to the credit reporting agencies. (You must review your state's requirement(s) and/or credit bureau requirement(s) for the specific document(s) to be submitted.)

For Massachusetts residents: The fee for each placement of a freeze, temporary lift of a freeze, or removal of a freeze is $5.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

Reporting of identity theft and obtaining a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

Kroll

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services[1] from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you'll receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You'll receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

[1] Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. To receive credit 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.