LEWIS THOMASON

Suite 2900, One Commerce Square
40 South Main Street
Memphis, TN 38103
T: (901) 525-8721 F: (901) 531-8514

Jutin N. Joy
DL: (901) 577-6105
JJoy@LewisThomason.com

December 2, 2020

Gordon J. MacDonald
Attorney General
attorneygeneral@doj.nh.gov
New Hampshire Department of Justice

RE: ***Notification of data security breach — Southern College of Optometry (Memphis, Tennessee)***
Date of Security Breach: February 7, 2020–May 20, 2020
Date of Discovery of Security Breach: October 21, 2020
Our file: S136M-00010

Dear Attorney General MacDonald:

This law firm represents the Southern College of Optometry (SCO) in Memphis, Tennessee. In providing this notification, as well as any subsequent information, respectfully, SCO reserves and does not waive any rights or defenses as to the applicability of New Hampshire law as to SCO, specifically including but without limitation to, the applicability of the state's data incident notification statutes, or personal jurisdiction.

On October 21, 2020, as part of its investigation into a data security incident involving a third-party, Blackbaud, Inc. ("Blackbaud"), as described below, SCO discovered that personal information of **one (1) New Hampshire resident** may have been involved in the incident.

As noted in media reports in recent months, Blackbaud, a leading software company serving thousands of educational institutions and other non-profit organizations around the world, experienced a data security incident earlier this year. SCO is a Blackbaud customer, and SCO has been closely following developments related to the investigation into the incident. Based on information SCO previously received from Blackbaud, SCO understood that SCO's data was protected by data encryption and was not involved by the incident. On September 29, 2020, however, SCO was informed by Blackbaud that some of SCO's data maintained by Blackbaud was not encrypted as previously thought, and that data may have been involved in the security incident.

Upon receiving this information, SCO immediately began its own investigation to determine what data pertaining to SCO constituents may been involved in the incident and requested additional information from Blackbaud. On October 21, 2020, SCO determined that information pertaining to one (1) New Hampshire resident may have been contained in a database impacted by Blackbaud's security incident. From SCO's investigation and based on information provided to SCO from Blackbaud, information contained in the impacted database

included name, address, and Social Security number. For some individuals, dates of birth and telephone numbers were also contained in the database. Although Blackbaud has reported to SCO that it has no reason to believe that any data involved in the incident was or will be misused, SCO is providing notice by mail to affected individuals. SCO expects notified individuals received their notice in the mail by the week of November 23, 2020. A template of the notification sent to the affected individuals accompanies this letter.

Blackbaud worked with cybersecurity experts and law enforcement to investigate the incident. Based on its investigation, Blackbaud determined that an unauthorized party gained access to its network between February 7, 2020 to May 20, 2020. During this time period, a copy of data files containing information from its customers, such as SCO, had been taken from its network. Blackbaud took steps to obtain confirmation that the files removed from its network had been destroyed. SCO's vendor has also informed SCO that, as a precautionary measure, it has been monitoring the internet for any evidence of disclosure of the information involved, and it has not found any indication of the information being available. Blackbaud has confirmed to SCO that it has made arrangements to provide affected individuals with 24-month, one bureau complimentary credit monitoring services. Additionally, SCO has been assured that Blackbaud has taken and continues to take steps to help avoid a similar situation from occurring in the future, including implementing additional safeguards such as encryption.

Should you have any questions or need any additional information, please do not hesitate to contact me at the email address or telephone number above.

Sincerely,

LEWIS THOMASON

Justin N. Joy

Attachment

Southern College of Optometry

November < >, 2020

<<<addressee first>>> <<<addressee middle>>> <<<addressee last>>>
<<<address line 1>>>
<<<address line 2>>>
<<<city>>>, <<<state>>> <<<ZIP>>>

Dear <<<FIRST>>>:

At Southern College of Optometry, we take protecting the security of our student and alumni data seriously, whether that data is maintained by us or by one of our vendors. We are providing you with this notice about a data security incident impacting one of our vendors which we recently learned may have involved some of your personal information.

As you may have seen in media reports in recent months, Blackbaud, a leading software company serving thousands of educational institutions and other non-profit organizations around the world, experienced a data security incident earlier this year. SCO is a Blackbaud customer and we have been closely following developments related to the investigation into the incident. Based on information we previously received from Blackbaud, we understood that SCO's data was protected by data encryption and was not involved by the incident. On September 29, 2020, however, we were informed by Blackbaud that some of SCO's data maintained by Blackbaud was not encrypted as previously thought, and that data may have been involved in the security incident.

Upon receiving this information, SCO immediately began its own investigation to determine what data pertaining to any current or former SCO students may been involved in the incident and requested additional information from Blackbaud. On October 21, 2020, we determined that your information was contained in a database impacted by Blackbaud's security incident. From our investigation and based on information provided to us from Blackbaud, information contained in the impacted database included your name, address, and Social Security number. For some individuals, dates of birth and telephone numbers were also contained in the database. Although Blackbaud has reported to us that it has no reason to believe that any data involved in the incident was or will be misused, please read the following additional information about the incident, as well as steps you can take to address any concerns about your information.

Blackbaud worked with cybersecurity experts and law enforcement to investigate the incident. Based on its investigation, Blackbaud determined that an unauthorized party gained access to its network between February 7, 2020 and May 20, 2020. During this time period, a copy of data files containing information from its customers, such as SCO, had been taken from its network. Blackbaud took steps to obtain confirmation that the files removed from its network had been destroyed. Our vendor has also informed us that, as a precautionary measure, it has been monitoring the internet for any evidence of disclosure of the information involved, and it has not found any indication of the information being available. Blackbaud has confirmed to us that it has made arrangements to provide you with complimentary credit monitoring services. Please read the enrollment information below. Additionally, we have been assured that Blackbaud has taken and continues to take steps to help avoid a similar situation from occurring in the future, including implementing additional safeguards such as encryption.

Complimentary Credit Monitoring Service

Blackbaud is providing you with access to Single Bureau (Experian) Credit Monitoring services by CyberScout at no charge. Services are for 24 months from the date of enrollment. If you enroll, when changes occur to your Experian credit file, notification is sent to you the same day the change or update takes place with

the bureau. In addition, Blackbaud is providing you with proactive fraud assistance to help with any questions you might have. In the event you become a victim of fraud, you will also have access to remediation support from a CyberScout Fraud Investigator. In order for you to receive this credit monitoring and other services, you must enroll within 90 days from the date of this letter. To utilize these services at no charge, visit the following web address: www.cyberscouthq.com/[redacted] If prompted, please provide the following unique code to gain access to services: [redacted]. Once registered, you can access monitoring services by selecting the "Use Now" link to fully authenticate your identity and activate your services. Please ensure you take this step to receive your alerts.

Directions for Placing a Fraud Alert and Other Information

Additionally, you may choose to adopt an increased level of protection by placing a fraud alert on your credit file at the three major credit bureaus. A fraud alert is a consumer statement added to your credit report. This statement alerts creditors of possible fraudulent activity within your report as well as requests that they contact you prior to establishing any accounts in your name. Once the fraud alert is added to your credit report, all creditors should contact you prior to establishing any account in your name. An initial fraud alert lasts one year. You may also place a credit freeze, also known as a security freeze, on your credit file which generally blocks access to your credit report. However, setting a credit freeze may delay your ability to obtain credit because lenders will not be able to view your credit report. Contact information for the three major bureaus is provided below:

Equifax (equifax.com)	Experian (experian.com)	TransUnion (transunion.com)
1-888-298-0045	1-888-397-3742	1-888-909-8872
PO Box 105788	PO Box 9554	PO Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094

As a general matter, you should remain vigilant about protecting your personal information by regularly reviewing financial account statements and credit reports. The Federal Trade Commission (FTC) recommends that you check your credit reports periodically in an effort to identify issues. You may obtain a free credit report annually from each of the three major credit bureaus by calling 1-877-322-8228 or by visiting www.AnnualCreditReport.com. You should promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the FTC. For more information about identity theft, other forms of financial fraud, and information about fraud alerts and security freezes, you can contact the FTC online at www.ftc.gov/idtheft; by mail at Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580; or by calling 1-877-ID-THEFT (438-4338).

We also encourage you to exercise caution regarding communications if you receive an unsolicited call or email about this incident. Even though such calls or emails may appear to come from a known, trusted source, these schemes are part of the growing trend of cybercrime impacting all types of organizations and individuals every day. Please know that SCO will not call or email anyone requesting any personal information as a result of this incident.

Again, SCO takes the protection of student and alumni data seriously, and we regret any inconvenience or concern this unfortunate incident may cause you. If you have any questions or for additional information, please contact George C. Miller, Vice President for Institutional Advancement, at 901-722-3217 or gmiller@sco.edu.

Sincerely,

Lewis N. Reich, OD, PhD
President