Southern College of Optometry

July 16, 2018

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

ACTIVATION CODE: <<< code >>>

Dear <<<addressee first>>>:

As stated in our email of June 15, 2018, we discovered that an SCO employee's email account was hacked that same day. Although we do not have any evidence that any misuse of personal information has occurred as a result of this incident, there was an email in the employee's email account which contained a list of students who had received student loans. As stated earlier, this list contained the student names, loan amounts, and Social Security numbers. From our investigation, it appears that the email containing this information was forwarded by the hacker to a third party email address.

We take the protection of our students' information seriously, and we have taken steps to help avoid a similar situation from occurring in the future. We also want you to read the information contained in this letter to protect your information from potential misuse not only in response to this notice, but as a general matter, given the unfortunate, but growing prevalence of identity theft in today's world.

Complimentary Credit Monitoring Service

Additionally, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (myTrueIdentity) for one year provided by TransUnion Interactive, a subsidiary of TransUnion® one of the three nationwide credit reporting companies. To enroll in this service, go to the myTrueIdentity website at www.mytrueidentity.com and in the space referenced as "Enter Activation Code," enter the following unique 12-letter Activation Code at the top of this letter and follow the three steps to receive your credit monitoring service online within minutes.

If you do not have access to the Internet and wish to enroll in a similar offline, paper based, credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at 1-855-288-5422. When prompted, enter the following 6-digit telephone pass code { } and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and September 30, 2018. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion, or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score. The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The service also includes access to an identity restoration program that provides assistance in the event your identity is compromised to help you restore your identity and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

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 90 days. You may also place a security freeze, or credit freeze, on your credit file which is designed to prevent credit, loans, and services from being provided in your name without consent. However, setting a security freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. Contact information for the three major bureaus is provided below:

Equifax (equifax.com)	Experian (experian.com)	TransUnion (transunion.com)
1-888-766-0008	1-888-397-3742	1-888-909-8872
PO Box 105788	PO Box 9554	PO Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016

As a general matter, you should remain vigilant about protecting your personal information by regularly reviewing financial account statements and credit reports to determine if there is suspicious activity such as new accounts being opened in your name. 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). The Vermont Attorney General's website, ago.vermont.gov, also has helpful information about fighting identity theft.

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 source, these schemes are part of a growing trend of cybercrime that impacts 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 situation.

We regret any inconvenience or concern this unfortunate incident has caused you. Please take the steps set forth in this letter to help protect yourself from identity theft or other misuse of your information, not only in response to this notice, but also as a routine practice, given the general prevalence of identity theft.

If you have any questions or for additional information, please contact Janine Tenorio, in the SCO Information Services department, 901-722-3202 or jtenorio@sco.edu.

Sincerely,

Lewis N. Reich, OD, PhD
President