July 30, 2015

Gus Castellanos
OCEA Communications Director
830 N. Ross St.
Santa Ana, CA 92701
800-548-9776

At the Orange County Employees Association, our first and most important commitment is to our members. The confidentiality of personal information is a critical part of that commitment. Regrettably, we recently learned that OCEA has been the victim of a cyber attack that may have put at risk some of the personal information of OCEA members, certain non-members, OCEA Health & Welfare Trust participants, OCEA staff, customers of Velece Corporation and dependents of any of these individuals.

We have no direct, conclusive evidence that personal information of our members or others actually has been taken from our systems. Given the apparent duration and methodology of the attack, however, as part of our commitment to you, and in an abundance of caution, we are notifying you and taking other proactive steps to protect your personal information going forward.

It has been publicly reported that, since 2005, more than 850 million records have been compromised in data breaches. Just since January of this year cyber attacks have occurred at UCLA Health Systems, United Airlines, Chick fil-A, Anthem, Toys r'Us, Microsoft, Starbucks, the United States Office of Personnel Management and Internal Revenue Service, and against numerous other victims, public and private, large and small. No one is immune.

On July 23, 2015, we determined that one or more attackers had successfully penetrated parts of the OCEA network and potentially gained access to personal information, including yours, that may have included: name, address, date of birth, Social Security number, driver's license number, payroll information, dental, vision, life and disability enrollment information, retirement status, information concerning dependents and usernames and passwords. The ongoing investigation suggests that the attack has been underway since at least June 5, 2015.

Upon learning of this potential compromise of personal data, we immediately notified the United States Secret Service and retained expert outside cybersecurity experts to assist us both with an investigation into the attack and, importantly, in taking measures to help protect against ongoing or future cyberattacks. The Secret Service quickly sent expert personnel to OCEA's offices and has now collected and analyzed data from our servers, but this notification was not delayed as a result of the Secret Service's involvement. We are notifying the Attorney General of California as well.

We are reaching out to you to provide you with information about this cyber attack and to notify you of the steps we are taking to protect you and steps you can take to protect yourself.

We have made arrangements to provide individuals potentially impacted with one year of free credit monitoring and identity theft recovery and restoration services, including up to $1,000,000 in identity protection insurance **at no cost to you** if you so choose. The coverage is through a national identity protection company. A letter should arrive at your mailing address by Monday, August 10, 2015, which will list any members of your household potentially impacted.

To enroll in and take advantage of the free services, visit or call them toll free at
The last day to take advantage of this offer by submitting an application will be October 30, 2015. You will need to reference the following access code when calling or enrolling on the website, so please do not discard this letter.
Your access Code is:

We urge you to enroll . In any event, there are steps you can take to help protect yourself. Upon request, any of the three nationwide credit reporting companies can place a free fraud alert in your file to alert potential creditors that you could be a victim of identity theft. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you.

A fraud alert will help prevent someone from opening new accounts in your name. As soon as one credit reporting bureau confirms your fraud alert, the others are automatically notified to place fraud alerts as well. All three bureaus will mail you confirmation letters and you will be able to order complimentary credit reports for review.

You may create a fraud alert by visiting www.Experian.com/fraud/center.html.

You will answer some questions to confirm your identity, and then a 90-day fraud alert will be added to your credit file. Experian will give you access to view your report online. You should examine it carefully for accuracy. If you contact Experian they will share this information with Equifax and TransUnion, which will each mail you confirmation letters containing a number to call to order complimentary copies of your credit reports for review.

You can also contact any of these credit agencies by a toll-free call as follows:

Equifax: 1-800-525-6285
P.O. Box 740241
Atlanta, GA 30374

Experian: 1-888-397-3742
P.O. Box 2104
Allen, TX 75013

TransUnion: 1-800-680-7289
P.O. Box 2000
Chester, PA 19022

You will not be charged for this service, but placing a fraud alert may delay your ability to open new sources of credit quickly.

We are making reasonable efforts to contact all individuals for whom we believe we possess what we believe to be current contact information. In the event you receive this notice and have dependents listed above who should be personally notified, please have them contact OCEA, Monday through Friday between 8:00 a.m. and 6:00 p.m. Pacific Standard Time at 800-548-9776, our dedicated cyberattack telephone number.

We apologize for any concerns or inconvenience this incident may cause you and want to provide you with as much information and support as we can. We will send you additional information about this incident if and as we get it and you can check "Frequently Asked Questions" at (www.oceamember.org/cybersecurity), or you may also call us Monday through Friday between 8:00 a.m. and 6:00 p.m. Pacific Standard Time at 800-548-9776.

In solidarity,

Jennifer Muir
OCEA General Manager