Client Memorandum

To: All Pension Plans

From: Klausner, Kaufman, Jensen & Levinson

Date: July 2019

Re: Cyberattack and Cyber Liability Insurance Coverage

The purpose of this memo is to heighten awareness of the possibility of a cyberattack for retirement plans and the importance of carrying cyber liability insurance. The Federal Bureau of Investigation warns that "state and local governments can be impacted by ransomware, an insidious type of malware that encrypts, or locks, valuable digital files and demands a ransom to release them." Several Florida municipalities have already been hit by cyberattacks; these attacks have cost hundreds of thousands of dollars to fight, or alternatively, to pay the requested ransom. Ill-prepared retirement plans are extremely vulnerable to devastating cyberattacks. Because there is never a good time for a cyberattack, bridging the gap early between attack and recovery is paramount.

Bridging the Gap Between Attack and Recovery:

Segal Consulting ("Segal"), a firm dedicated to providing services to retirement plans and other public sector clients, recommends creating an "incident response plan" to combat a cyberattack or strike. According to Segal, an incident response plan should consist of three major components: (a) contain, (b) eradicate, and (c) recover from the incident. Segal also suggests taking the following preparatory steps to assist with cyberattack recovery:

1. Create a list of critical business functions;

2. Identify when those critical business functions are during the calendar year and how much time they usually take to complete; and

3. Identity the criteria used to determine if alternate arrangements must be made to meet your critical business obligations.

A carefully crafted incident response plan can help retirement plans address the problems experienced after a cyberattack and work swiftly to find a resolution. A good plan is essential for business continuity. Ensuring business continuity during a cyberattack can help a retirement plan maintain its critical functions at all times, except after a major disaster.

Other ways to prepare for a cyberattack include backing-up all computer networks and securing alternate methods to have retirement benefits timely processed. Such alternate methods may include contracting with an off-site third-party to handle the processing of retirement benefits in the event of an emergency. All retirement plans should reach out to plan sponsors seeking the procedures it has in place in the event of a cyberattack.

Cyber Liability Insurance:

We recommend that all retirement plans require vendors to have or to purchase cyber liability insurance in the amount of $5,000,000.00. All current agreements with vendors that do not already include cyber liability insurance should have the policy amended to include a cyber liability rider adding such coverage. We also recommend adding the following language, or similar language, to all vendor contracts:

> The vendor agrees to obtain and maintain in full force and effect under the terms of this Agreement, at least a $5,000,000.00 cyber liability policy. The policy shall include coverage for breach response expenses, security and privacy liability, regulatory investigation coverage for covered losses resulting from a data breach of related claims. The vendor will endeavor to notify the Board, in writing, in the event of any change in its cyber liability policy and to immediately notify the Board if said insurance is terminated, canceled or discontinued, in whole or in part. The vendor agrees to periodically provide confirmation to the Board that coverage continues. The vendor will add the Board as an additional insured.

This language will be included in vendor agreements drafted by our office on the retirement plan's behalf.

Section 501.171, Florida Statutes, governs "security and confidential personal information." Under this statute, a governmental entity is considered a "covered entity"

and must take steps to notify those affected by a cyberattack and to "restore the reasonable integrity of the data system that was breached." Section 501.171(4), Florida Statutes, provides:

> [A] covered entity shall provide notice to each individual in this state whose personal information was, or the covered entity reasonably believes to have been, accessed as a result of the breach. Notice to individuals shall be made expeditiously as practicable and without unreasonable delay, taking into account the time necessary to allow the covered entity to determine the scope of the breach of security, to identify the individuals affected by the breach, and to restore the reasonable integrity of the data system that was breached, but no later than 30 days after the determination of a breach or reason to believe a breach occurred unless subject to a delay authorized. . .

Florida Statute, Section 501.171, may be read in its entirety at http://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&Search_String&URL=0500-0599/0501/Sections/0501.171.html.

The Federal Trade Commission provides a useful guide outlining steps an organization should take after a breach has occurred. This guide can be accessed by clicking the following link: https://www.ftc.gov/system/files/documents/plain-language/pdf-0154_data-breach-response-guide-for-business-042519-508.pdf.

Any retirement plan in need of assistance choosing a cyber liability insurance policy may contact James Martinez, with Gallagher at James_Martinez@ajg.com. Gallagher has developed a cyber liability insurance program with the National Conference on Public Employee Retirement Systems ("NCPERS"). NCPERS membership is not required for assistance with this matter.

For additional information concerning new developments in cyber security policy please contact John Reidy, with the Pension Technology Group at john@ptg-usa.com or by telephone at (617) 977-8408, ext. 18.

As always, feel free to contact our office if you have any cyberattack or cyber liability insurance questions.