Segal Consulting

1920 N Street NW Suite 400 Washington, DC 20036-1659
T 202.833.6400 www.segalco.com

MEMORANDUM

To: City of Los Angeles Deferred Compensation Plan
Board of Deferred Compensation Administration Meeting

From: Wendy Young Carter

Date: September 6, 2016

Re: **Document Imaging and Security**

Imaging and Document Storage

Data management of one of the most critical aspects of defined contribution retirement plan administration and recordkeeping. Often **document imaging** is confused with "going paperless." And, while technologies like scanning can certainly be used to digitize paper, the digitization is not the end in itself. The real benefit of a document imaging system is how it improves business processes such as plan and participant recordkeeping and administration. The benefit of a document imaging used in a workflow system is that it can create more efficient and accurate processes which benefit the City and its plan participants.

Document imaging is the process of scanning and identifying paper documents so the documents can be viewed, managed, and acted upon online. These documents could be files already saved in a computer readable format or files created from scanned paper documents (where the point of origin can be the mailroom or sent from local offices such as the City's). The document imaging process images and converts paper files to electronic images which are then housed through a secure, web-based document management system (DMS), or what many call a "virtual file cabinet." Once the images are uploaded into the secure system, with just a click of a mouse, service provider personnel (including call center or local representatives) can access information.

Workflow is the process for managing the imaged documents. For example, for the City's Plan a variety of transactions, such as a distribution request or a request to change a contribution amount, can be submitted via a paper form. In its simplest form, workflow is the process that takes that imaged form and sends it through an electronic routing, review, approval and execution process.

While there are a variety of benefits including always having instant access to information, document security is still vital. A DMS provides better control over sensitive documents and there is less chance for documents to be lost or misfiled. Access to documents can be controlled for different groups or individuals. In addition, a DMS leaves an audit trail of who has viewed a document, when it was accessed, and how it may have been modified. Managed documents are traceable and can be tagged to allow for automated alerts. A user can determine who has viewed

it, when, and how often. Workflow tasks can be set up, for example, to automatically notify a user that a document is waiting for approval and a notification can be sent if no action is taken within a pre-determined amount of time. Tasks may be placed in the workflow queue with normal, high, or urgent priority and notes can be added.

In terms of the selection process both firms are required to image and store all documents for the duration of the firm's contractual relationship with the City's Plan and to transmit them to a future service provider. Both firms confirmed their acceptance of these requirements although Empower indicated it would negotiate the terms for the requirements with the City and indicated a $150 hourly rate for the file export process.

Security Protocols, Disaster Recovery and Guarantees

Retirement plan recordkeepers receive, keep and maintain large amounts of personally identifiable data and access to financial accounts. They are a repository of sensitive personal information such as Social Security numbers, dates of birth, addresses, as well as a participant's designated beneficiary and his or her personal information. The Plan's account and transactional information not only needs to be stored but it also needs to be accessed as part of providing recordkeeping services including providing access not only to the recordkeeper's staff but to plan sponsors and their participants.

Identity theft and sensitive information falling into the wrong hands are things all businesses work hard to prevent. Data is always subject to being compromised in a variety of ways and firms use a variety of methods to reduce this risk. As a result, the RFP issued addressed many of these areas. As required, both firms certified that they would:

- Confidentially maintain participant data, records and personal information such as social security numbers, dates of birth, marital status, home addresses, contribution and account balance information, investment information, transaction histories, and other information related to participation in the Plan.

- Indemnify the City for any liability associated with security breaches of the recordkeeping system. Note that Empower added language clarifying that the indemnification would be only for losses actually and reasonably incurred by or imposed on the City to the extent arising out of or resulting from Empower's negligence or willful misconduct in its performance under the Agreement.

Both firms provided information to the questions about resources and policies. It is important to note that both firms have security policies, conduct SSAE audits, which include evaluating security, and comply with ISO 27001. In addition, the defined contribution recordkeeping industry is evaluating additional ways to provide assurance that reasonable and effective security efforts are being made. It is important to comment that physical security and protocols, such as password requirements and removing credentials immediately upon employee termination are very important. Other areas include how data is secured especially when being transmitted or received. Both firms provided their disaster recovery policies.

Each firm was asked to describe its response plan in the event of a data security breach. Empower described their information security program from a high level. Voya's response was also general but did indicate that it has not suffered a security breach of any materiality and for in the limited instances where there had been unauthorized disclosures of participant data (such as mailing errors or misdirected emails), immediate action was taken to notify the plan sponsor.

As most people are aware, data breaches often include providing free credit monitoring to affected individuals. Both firms responded affirmatively that such coverage was provided. As is typical this protection is included in Empower's cyber-liability insurance policy which provides coverage for, among other things, privacy breach notification costs and includes coverage for costs incurred to notify any third party of a security failure or privacy event, including the provision of credit monitoring services or identity theft insurance. Voya also indicated it would provide free credit monitoring when appropriate.