Negotiating Cybersecurity Contractual Protections for Retirement Plans

By Jeffrey D. Hutchings, Susan P. Serota and Jessica Lutrin

This alert also was published as a bylined article on Law360 on June 3, 2016.

The ERISA Advisory Council[1] recently announced that, as part of its goals for 2016, it will be focusing on cybersecurity issues affecting retirement plans and, in particular, the extent to which such issues relate to third-party administrators and vendors (TPAs) of retirement plans. By shining the spotlight on the role of TPAs in combatting cyber-related threats to retirement plans, this announcement demonstrates that retirement plan sponsors would be well-served to proactively assess the cyber risk profiles of their retirement plans. Specifically, retirement plan sponsors should focus on developing and implementing a comprehensive and effective risk management strategy that includes, among other actions, the implementation and periodic review of contractual protections in arrangements with their plans' TPAs.

This advisory is the second in a series of advisories dedicated to understanding cybersecurity issues.[2]

Contractual Landscape

Most contracts prepared by TPAs for recordkeeping and related services do not provide adequate contractual protections relating to data security. Typically, the TPA's form contract contains minimal or no protections and, in some cases, there are more obligations imposed on the plan sponsor relating to data security (e.g., protection of personal identification numbers of plan participants) than on the TPA. Indeed, a literal reading of the general indemnification provisions of some form contracts would require the plan sponsor to indemnify the

[1] The ERISA Advisory Council (which is composed of members who are representatives of employers, employee organizations, the general public and the fields of insurance, accounting, corporate trust, actuarial counseling, investment counseling and investment management) advises the Secretary of Labor on carrying out her responsibilities under the Employee Retirement Income Security Act of 1974.

[2] For part one, see An Overview of Cybersecurity Issues Affecting Retirement Plans.

TPA against losses arising from a cybersecurity breach on the TPA's systems in the absence of gross negligence or willful misconduct by the TPA.

This is not surprising. Many of the contract forms were developed many years ago before cybersecurity issues attracted significant attention. While TPAs update their forms from time-to-time, it is not in their interest to offer robust contractual commitments in this area. As a result, it is incumbent on plan sponsors to raise the issue with their TPAs and propose appropriate contractual protections.

Key Contractual Protections

We recommend that plan sponsors and/or plan administrators seek the contractual protections set forth below. The types of contractual protections can be broken down into the following four categories: (i) protection of data, (ii) restrictions on the use and location of data, (iii) responses to actual or threatened cybersecurity breaches and (iv) liability and risk allocation.

Data Protection Safeguards

The contract should require the TPA to commit to maintain appropriate safeguards for plan participant data. Typically, these commitments include some combination of the following:

- *Compliance with TPA Policies* – The TPA should commit to comply with its own cybersecurity policies and agree not to materially degrade the level of security reflected in those policies during the term of the contract. Plan sponsors and/or plan administrators should request copies (or at least summaries) of the TPA's policies and have their internal IT security personnel review them from a due diligence perspective.

- *Compliance with Applicable Law* – The TPA should commit to comply with all U.S. and foreign data security and privacy laws applicable to the TPA's services.

- *Compliance with Industry Standards* – The TPA should commit to meet industry standards relating to data security. For example, the International Organization for Standardization (ISO), which is an international standard-setting body, publishes information security standards codified in ISO 27001 / 27002. It would be reasonable to require that the TPA agree to comply with these standards and maintain ISO 27001 certification.

- *Security Audits* – The TPA should commit to have a nationally recognized independent third party conduct annual (or more frequent) audits or reviews of the TPA's cybersecurity practices at facilities used to deliver the services and provide a copy (or at least a summary) of the audit report to the plan sponsor. One of the more common types of audit reports furnished by service providers is a SOC 2, Type II report under Attestation Standards Section 101 published by the American Institute of Certified Public Accountants. The SOC 2, Type II audit addresses the operating effectiveness of the TPA's controls relating to security, availability, processing integrity, confidentiality and privacy.

With possible exceptions for certain large transactions, plan sponsors and/or plan administrators should not expect TPAs to agree to comply with the cybersecurity policies of the plan sponsor and/or plan administrator. Recordkeeping and similar services provided by TPAs are "one-to-many" solutions—that is, from a data security standpoint, the solution is generally the same for each client. Plan sponsors and/or plan administrators will need to conduct due diligence of the TPA's cybersecurity practices and procedures to provide a level of comfort that plan participant data is appropriately protected.

Restrictions on Use and Location of Data

The contract should include the TPA's commitment to use plan participant data solely to provide services to the plan sponsor and/or plan administrator and plan participants with possible exceptions for:

- The TPA's use of anonymized, aggregated data for research, analysis, white papers, etc.; and
- The TPA's provision of other products or services to plan participants *but only if* the participant expressly authorizes the use of his or her data for this purpose.

The location of participant data should be restricted to specified countries or advance notice of any change should be required to be given by the TPA to the plan sponsor and/or plan administrator with an opportunity to terminate the contract without liability if the plan sponsor and/or plan administrator is uncomfortable with the new location. For example, the plan sponsor and/or plan administrator may have concerns with offshore personnel of the TPA or its affiliates in certain countries (e.g., India) having access to plan participant data or want access limited to remote screen access without any ability to download, copy, print or transfer any data. In addition, transfers of participant data by the TPA from the European Union to the United States could present legal compliance issues that the plan sponsor and/or plan administrator will want assurance are being properly addressed by the TPA.

Response to Cybersecurity Breaches

The contract should require the TPA to respond to any data security breach (or a reasonable suspicion of a breach) that may impact plan participant data in an appropriate manner. This would include commitments by the TPA to:

- Promptly notify the plan sponsor and/or plan administrator of the breach (typically within 24 hours, unless otherwise directed by law enforcement);
- Investigate the breach with the plan sponsor's and/or plan administrator's participation (if desired by the plan sponsor and/or plan administrator) and preserve evidence;
- Perform a root cause analysis of the breach and prepare an action plan to remediate it;
- Remediate the breach and use all commercially reasonable efforts to prevent its recurrence; and
- Keep the plan sponsor and/or plan administrator apprised of ongoing developments and cooperate with the plan sponsor and/or plan administrator in addressing legal compliance and other issues relating to the breach.

Liability and Risk Allocation

Cybersecurity breaches can have devastating financial consequences. The *2015 Cost of Data Breach Study: United States*, published by the Ponemon Institute, indicates that the total average cost paid by organizations as a result of a cybersecurity breach is approximately $6.5 million. Therefore, it is important that the contract hold the TPA liable for cybersecurity breaches, at least in circumstances where the TPA has been negligent or failed to comply with its contractual commitments relating to data security.

Because of the substantial financial exposure associated with cybersecurity breaches, TPAs may be unwilling to accept unlimited liability in this area. The TPA may seek to exclude recovery of consequential damages (e.g., lost revenues and profits, reputational injury, etc.) by the plan sponsor and/or a cap on liability for cybersecurity breaches. While unlimited liability may not always be achievable, it is reasonable for plan sponsors and/or plan administrators to expect that:

- Specified types of costs associated with a cybersecurity breach will be recoverable by the plan sponsor and/or plan administrator, such as reasonable forensics/investigation/legal costs, fines and penalties, compliance with breach reporting laws, and credit monitoring;
- The TPA will fully indemnify the plan sponsor and/or plan administrator against any claims of plan participants and other third parties; and
- Any cap on liability will be set at a high enough level to permit recovery of all or a substantial portion of the potential costs likely to be incurred by the plan sponsor and/or plan administrator in the event of a cybersecurity breach.

Negotiating Contractual Protections

Of course, it is much easier to identify contractual protections than to obtain them. Like any service provider, TPAs are resistant to agreeing to robust contractual commitments that could result in substantial liability to their enterprise. In addition, a plan sponsor's and/or plan administrator's ability to secure these commitments will be a function of its negotiating leverage. A plan sponsor with a large employee base in which multiple TPAs are competing for the business is more likely to achieve the outcomes described above than a small or medium-sized plan sponsor negotiating with a TPA on a sole source basis.

As such, the negotiating strategy for any particular transaction will need to be developed on a case-by-case basis in light of the size of the transaction and the plan sponsor's and/or plan administrator's objectives and priorities, including the amount of time and effort the plan sponsor and/or plan administrator is prepared to dedicate to securing data security protections. As a general matter, however, the following approaches may be helpful to plan sponsors and/or plan administrators in achieving favorable outcomes in both large and small transactions:

- *Identify Cybersecurity Requirements Early in the Process* – This signals to the TPA the importance of the issue to the plan sponsor and/or plan administrator and compels the TPA to respond to the requirements early in the process when the plan sponsor and/or plan administrator has the greatest negotiating leverage.
- *Maintain Competition* – Like any service provider, TPAs do not want to lose business (regardless of the value) to their competitors. Therefore, plan sponsors and/or plan administrators should consider either a competitive procurement process or starting a sole source procurement early enough to provide a credible threat of terminating negotiations with the TPA if it fails to meet key requirements of the plan sponsor and/or plan administrator.
- *Leverage Precedent* – Each transaction between a TPA and a plan sponsor and/or plan administrator is confidential, and a TPA is not bound to offer client "A" the same contractual protections as client "B." However, it is often easier for a TPA to secure internal approval for a contractual provision in cases where the TPA has agreed to a similar type of provision in a prior transaction. Plan sponsors and/or plan administrators can benefit from outside counsel leveraging their prior experience with a TPA in negotiating and drafting contractual protections that will be acceptable to the TPA.

If you have any questions about the content of this advisory please contact the Pillsbury attorney with whom you regularly work, or the authors below.

Jeffrey D. Hutchings (bio)
Washington, DC
+1.202.663.8163
jeffrey.hutchings@pillsburylaw.com

Susan P. Serota (bio)
New York
+1.212.858.1125
susan.serota@pillsburylaw.com

Jessica Lutrin (bio)
New York
+1.212.858.1090
jessica.lutrin@pillsburylaw.com

Pillsbury Winthrop Shaw Pittman LLP is a leading international law firm with 18 offices around the world and a particular focus on the energy & natural resources, financial services, real estate & construction, and technology sectors. Recognized by *Financial Times* as one of the most innovative law firms, Pillsbury and its lawyers are highly regarded for their forward-thinking approach, their enthusiasm for collaborating across disciplines and their unsurpassed commercial awareness.