Addressing Cybersecurity in Your Retirement Plan TPA Contract

May 25 2016

Posted By: Timothy C. McDonald

Practice Area: Compensation and Benefits/ERISA & Information Technology, Data Privacy and Security

Employers are well aware of the prevalence of cyber-attacks. Attacks on Anthem, Target, Home Depot, the Internal Revenue Service, among others, make national headlines and the costs associated with data breaches can be significant for businesses. According to the *2015 Cost of Data Breach Study: United States*, conducted by Ponemon Institute LLC and sponsored by IBM, the average cost to an organization of a data breach is $6.5 million, and this study even excluded the cost of massive breaches, i.e., those involving more than 100,000 compromised records.

With the ever-increasing risk of cyber-attack, employers are focused upon the need to address cybersecurity with respect to their internal systems as well as their contracts with vendors. Cybersecurity, however, remains largely ignored in contracts with those providing services with respect to employer retirement plans. Proper due diligence demands that employers review the cybersecurity measures taken by their retirement plan service providers and the service contracts with those providers to assess and minimize exposure to liability for cyber-attacks.

Confidential Data and Access to Plan Assets. The third-party administrator ("TPA") that you retain to provide recordkeeping and other administrative services for your retirement plan (e.g., 401(k) plan, 403(b) plan, etc.) holds sensitive data regarding your employees. This data, referred to as "personal identifiable information" or "PII," may include social security numbers, addresses, dates of birth, account balance information, beneficiary information, and bank account information. In addition, your TPA may maintain systems that allow employees to initiate retirement plan transactions online. Your employees may be able to obtain plan loans and/or account withdrawals through your TPA's website. As a result, a successful cyber-attack against your retirement plan TPA could result in the theft of employees' identities or the theft of retirement plan assets. Hackers have (a) used online systems to access participant retirement plan accounts, change the account information, and direct distributions from the accounts to improper parties, and (b) accessed a TPA's participant database to steal personal data (e.g., names, addresses, social security numbers, etc.).[1]

Developing Law and Fiduciary Duties. The law governing cybersecurity is developing and is currently a patchwork of state and federal regulations. There is no comprehensive federal law governing cybersecurity. There are laws that govern the financial industry's use of financial information, e.g., the Fair Credit Reporting Act, Gramm-Leach-Bliley Act, and the Fair and Accurate Credit Transactions Act. These laws, however, do not apply directly to retirement plans or the PII held in conjunction with those plans. Most states have laws that address the protection of PII in some form but, like the federal laws, these laws do not apply directly to retirement plans.

The law related to the assessment of liability in the event an employee or former employee experiences a loss as a result of a cyber-attack on an employer's retirement plan(s) is also developing. Plan fiduciaries clearly have an obligation to protect retirement plan assets. Given that cyber-attacks may jeopardize the safety of those assets, employers should consider cybersecurity as it relates to the safety of plan assets when making decisions to select or retain a TPA and/or trustee for its plan(s).

It is less clear what the employer's exposure would be in the event an employee's identity would be stolen as a result of a cyber-attack on the retirement plan TPA if no theft of retirement plan assets occurs. It seems safe to assume, however, that an injured employee's counsel would want to examine the due diligence the employer undertook in selecting the TPA if, for example, the TPA's security measures fell below industry standards.

Data Security, Privacy, Contract Review, and Monitoring. If you have not done so, you should discuss with your TPA and other retirement plan service providers your privacy policy and data security plan to ensure that your retirement plan will be administered in accordance with the plan and policy. If you do not have a privacy policy or a data security plan for your retirement plan data, you will want to develop and implement one as soon as possible.

In addition, you should review the cybersecurity provisions of your contract with your retirement plan TPA. Despite the risk faced by an employer's retirement plan and employees as a result of a cyber-attack on a TPA, administrative service agreements with TPAs generally do not address cybersecurity specifically. This omission occurs for a number of reasons. If an employer has used the same TPA for a number of years, the service agreement may be old and predate the escalation in cyber-attacks. If no problems have arisen, the employer may not have thought there was a need to review the agreement. In addition, the TPA generally provides the service agreement form and does not have an incentive to address cybersecurity specifically in the agreement. Finally, some employers may view TPA agreements as form contracts and not realize these contracts often shift liabilities back to the employer and, therefore, need legal review.

If cybersecurity is not addressed or is only minimally addressed in your agreement with your TPA, we would propose an amendment to the contract. Among other provisions, the amendment could address:

- The TPA's agreement to keep PII in its possession both secure and confidential;
- The TPA's agreement to restrict access to, and the use of, PII;
- The TPA's agreement to maintain PII solely within the United States;
- A description of the data security safeguards the TPA agrees to implement and the standards it agrees to follow to prevent unauthorized access to plan accounts and to protect PII;
- The TPA's agreement to use industry best practices with regard to the storage of data;
- The TPA's agreement to conduct audits of its data security practices and to provide the results of those audits to you for review (e.g., by the IT professionals within your organization);
- Your right to review your TPA's security measures or perform a data security audit periodically;
- The TPA's agreement to notify you promptly of a data security breach (whether or not PII was compromised), comply with notifications requirements imposed by applicable law, and take steps to mitigate losses caused by the breach;
- The TPA's agreement to maintain insurance (e.g., cyber insurance) to provide some assurance that the TPA could financially survive the costs (and protect your interests in the event) of a data breach; and
- The allocation of liability in the event of a data breach.

[Note: If you are in the process of reviewing TPA services currently and you are sending out requests for proposal, we encourage you to require each TPA candidate responding to provide, with its proposal, a copy of any agreement it will ask you to sign. Your negotiating leverage is the greatest before you make your TPA selection. Far too often, we find that an employer who selects a new TPA first receives the service agreement from the TPA after the employer announces the selection, after the changes in TPA and plan investment funds have been communicated to employees, and on the eve of the scheduled transfer of plan assets to the new vendor(s). At this late stage, the employer's negotiating leverage has been significantly diminished.]

Finally, you should establish a procedure to review periodically your TPA's compliance with the data security and privacy provisions of your service contract and your TPA's compliance with its own data security and privacy cybersecurity procedures and policies.

Please contact the author or any von Briesen & Roper Compensation & Benefits attorney if you would like us to assist you in developing a cybersecurity policy for your retirement plan, assessing your retirement plan's cybersecurity risk, reviewing and amending your TPA contract(s), and/or establishing procedures to monitor your TPA's cybersecurity compliance.

[*Please note that a discussion of cybersecurity of health plan information is beyond the scope of this article. Please be aware, however, that various federal and state laws govern the privacy of health plan information. These laws include, for example, the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the Health Information Technology for Economic and Clinical Health ("HITECH") Act. Cybersecurity must also be assessed and monitored in relationships and contracts with health plan service providers. Please contact us if you would like more information.*]

[1] 2011 Advisory Council on Employee Welfare and Pension Benefit Plans report to the Secretary of Labor, titled "Privacy and Security Issues Affecting Employee Benefit Plans."

---

von Briesen & Roper Legal Update is a periodic publication of von Briesen & Roper, s.c. It is intended for general information purposes for the community and highlights recent changes and developments in the legal area. This publication does not constitute legal advice, and the reader should consult legal counsel to determine how this information applies to any specific situation.