ALERT

APRIL 2017

Data Breach Risks for 401(k) and Retirement Plans

There has been a recent spike in attacks on 401(k) and retirement plans by cyber criminals. Some have been reported publicly, and we are aware of several nonpublic incidents as well.

A data breach is a disruptive event. For plan fiduciaries, there are several factors that create heightened risk. First, an attack can result in loss of personally identifiable information and theft of funds. Recent incidents have seen cyber thieves empty accounts of plan participants, including C-suite executives. For business relations reasons, corporate plan sponsors have taken responsibility for making plan participants whole.

Second, plans use third-party service providers to administer accounts and handle data. Yet, plan fiduciaries may remain responsible for their actions under ERISA, and they are generally obligated to provide prudent oversight.

Third, because ERISA requires that claims by plan participants be asserted against the plan fiduciary, it is critical to have contractual specifications about data and plan assets security, and mechanisms to shift the loss to the service provider where circumstances warrant. Otherwise, disputes may arise over which party is responsible for cybersecurity.

In light of these risks, we offer the following recommendations for plan fiduciaries:

- Undertake a careful review of agreements with service providers. Contracts should make them responsible for cybersecurity and set standards for data protection consistent with ERISA and other laws, as well as up-to-date industry standards. In the event of a breach, contracts should provide plan fiduciaries with prompt notice, access to requested information, and indemnification against claims and losses.

- Obtain insurance that covers cyber theft and data breach risk. Some cyber policies will cover losses incurred by plan fiduciaries, including investigation expenses, notice costs, reimbursement of stolen funds, and defense of claims. But coverage varies greatly from insurer to insurer, and many policies contain problematic exclusions. It is important to understand the available coverages and to select policies that meet your needs.

- Should a breach occur, the plan fiduciary should take an active role in the response effort. A prudent "expert level" response will include diligent investigation, notice and protective measures for plan participants, and implementation of appropriate corrective measures.

Jones Day currently is assisting clients in responding to several nonpublic cyber incidents involving 401 (k) and retirement plans.

CONTACTS

John A. Vogt
Irvine

Travis DeHaven
Atlanta

Richard DeNatale
San Francisco

Todd S. McClelland
Atlanta