Retirement Plan Fiduciary? Is Your Plan in the Crosshairs of Hackers?

In our ongoing quest to identify and prioritize meaningful corporate risk before it finds our client-partners' organizations and materially impacts their financial position, or worst yet, exposes them to personal liability, this article will shed light on one such significant emerging risk:

Retirement Plan Network Security

Most organizations in the United States sponsor qualified retirement plans, such as 401(k) or 403(b), for the benefit of their employees. The employer, as Sponsor of the plan appoints Fiduciaries, who have the duty to operate the plan with the skill and care of a prudent expert and solely in the best interest of its Beneficiaries (Participants).

In 1974, prior to the advent of the modern internet, Congress passed the Employee Retirement Income Security Act, 29 U.S.C. § 1101 et seq. (ERISA) to protect retirement plan assets by requiring Fiduciaries (Plan Trustees, Plan Administrators, members of a plan's Retirement Committee, etc.) to act prudently (duty of care, loyalty, obedience) and follow the terms of plan administration and governance documents. Fiduciaries who do not adhere to these conduct requirements may be personally liable to restore any losses to the plan, including investment losses.

Given the amount of assets in these plans, combined with the risk of personal liability, the potential exposure is real and significant, so let's look at a few scenarios in order to better understand the breadth and complexity of this emerging digital (aka "cyber") exposure.

Scenario One: The Plan Administrator's computer network is compromised (hacked) by a third party who successfully transfers $9,000 from each of your participants' accounts.

You would assume that the Plan Administrator would be liable since it was their computer system that was compromised. But when you look at the Plan's contract or cyber security guarantee presented during your onboarding meeting with the Administrator, you'll likely find:

1.) The Administrator has limited its liability.

2.) The contract may require mandatory arbitration by each participant.

3.) Then, when you reach out directly to the Administrator to inquire about the cyber security guarantee, you'll be re-introduced to the limited, conditional, non-insurance cyber security "protection" or "guarantee" the Administrator offers. You'll also learn, of course, that the Administrator has binding unilateral discretion regarding whether you're eligible for the protection or guarantee.

What are your options?

At this point, you'll probably come to the conclusion that litigation is the only way forward. But who has the right to litigate and who pays for legal counsel to pursue the Administrator? With the precedent set by Amaro v. Continental Can Co. in the mid 1980's, that ERISA claims are not arbitrable, one would assume it's the Plan Fiduciary's responsibility. But the plan has no assets besides the Participants' funds, which cannot be utilized to fund the litigation, and the plan's Fiduciary Liability insurance policy doesn't offer coverage for legal fees when the plan is the plaintiff. Rather than a class action by the plan, what if it was the individual plan Participant's obligation as was the case in August of 2019 when the Ninth Circuit reversed the district court's denial of a motion to compel arbitration (expressly agreed in the Plan document that all ERISA claims would be arbitrated) and ruled that the plaintiffs must individually arbitrate their fiduciary duty claims (poor performance/ excessive fees)?

© 2019 Andrew Robinson International Risk Management Consultants, Inc.

To compound things further, once you engage counsel, the conversation will include whether replenishing the assets to reduce the loss of investment income, prior to final adjudication, is advisable and feasible.

So, without another viable funding source, that leaves the Plan Fiduciaries (personally) or the Plan Sponsor to replenish the lost funds and to fund what will undoubtedly be a lengthy and expensive battle.

Scenario Two: The Plan Sponsor's network is compromised by a third party who then successfully transfers the full account balances of all your participants over 59½ years of age.

What are your recourse options?

If the Plan Sponsor's network is the source of the breach, then one of its corporate insurance policies should cover the loss, right? The quick answer is maybe, but probably not, as most Commercial Crime policies only cover theft if it involves the Sponsor's employees or Plan Fiduciaries, which is not the case here. Looking elsewhere in the Sponsor's corporate insurance portfolio, traditional Fiduciary Liability insurance policies are designed to cover errors and omissions in the administration of the plan, not the theft of plan funds, and most Directors' and Officers' Liability policies contain an ERISA exclusion. So-called Cyber insurance is also likely to come up short, as it's clear that segment of the insurance industry understands the enormity of the risk and most insurance brokers either don't know to include the Plan or don't push back on their underwriting partners to include it.

Scenario Three: A Plan Participant's account is compromised using the Participant's username/password and the unauthorized user takes the maximum loan from the Participant's account.

What are the options here?

In this scenario where the Plan Participant is apparently the cause of the compromise (breach), the Plan Participant's only avenues to recover may be their homeowner's/renter's insurance policy (probably a minimal privacy sub-limit, if available) or the goodwill of the Sponsor and/or Administrator to replenish the stolen funds.

Retirement Plan Network Risk Recap

All of the above scenarios will create a vexing time for everyone involved. When such losses occur, the conversation between the various interested parties typically starts off conciliatory, then, as the investigation phase gets underway, the tone quickly moves to finger pointing followed by each party hunkering down in a demonstration of Darwinian survival of the fittest (and most informed).

The reality in each of these scenarios is that the Beneficiaries need to be made whole (i.e. return of lost funds and loss of investment return/income during the period). So, the question is who's responsible for replenishing the Beneficiaries' funds/assets and will they have the ability and financial resources to do so, particularly when the losses are very large?

The magnitude of loss in some of the potential scenarios is staggering. Imagine if the malicious actor in Scenario One instead took $1,000 from every Plan Participant on the Administrator's network, not just from each of your Plan's Participants. Even if the Plan Administrator wanted to make everyone whole, it's highly unlikely they would have the assets and/or insurance limits to do so.

Now your thinking will likely transition to what you can do to protect your employees, Plan Fiduciaries, Board of Directors, and capital accounts of your organization.

To get a better handle on your organization's current Cyber/ERISA risk position, we suggest

© 2019 Andrew Robinson International Risk Management Consultants, Inc.

starting with a simple self-check, including answering the following questions:

- ✓ Do you provide Plan Beneficiaries with information and education on network security?
- ✓ Have you taken the correct steps to provide the Plan and its Fiduciaries a safe harbor?
- ✓ Does the Sponsor provide defense and indemnification to the Plan Fiduciaries?
- ✓ Do you know the level of cyber preparedness your plan's vendors are required to maintain?
- ✓ Do you know the types and limits of insurance your plan's vendors rely on for these types of events?
- ✓ Do you know the conditions your Administrator requires to be met for Plan Participants to obtain their (non-insurance) "protection" or "guarantee" for cyber breaches and loss of funds?
- ✓ Have you negotiated favorable "cyber" terms and requirements in your agreements with plan vendors and Administrators?
- ✓ Have you had legal counsel, or a licensed insurance advisor review your Crime, Fiduciary, and Cyber Liability policies?
- ✓ Does your Cyber policy cover your retirement plan(s) and theft of personally identifiable information and/or assets from a third party's network?
- ✓ Have you identified and perhaps even struck contingent service agreements with the vendors (IT Forensics, Public Relations, Legal, Notice Providers, Credit Monitoring, etc.) needed to respond successfully post event to these types of loss scenarios?

As you look at your organization's particular risk profile, you'll almost certainly come to the conclusion that this is a multidimensional and potentially catastrophic risk that requires outside professional support. Managing network risk and safeguarding personally identifiable information (PII) are complex and growing issues for all organizations. This, combined with the fact that ERISA preempts any state law that may apply to such plans, would probably turn this into a federal matter and/or the vendor contract may require each participant to arbitrate their loss individually, with either scenario adding to the potential cost and legal consequences.

The above scenarios and commentary, which are concerning enough as presented, focus mainly on the loss of funds and investment gains, but do not examine the impact the loss of PII can have on the Plan Sponsor, Fiduciaries, and Beneficiaries. While ERISA itself does not currently define PII to be an asset of the Plan or impose cyber security standards on Fiduciaries, the Department of Labor has provided guidance that Plan Administrators should take measures to protect the PII of the Plan's Beneficiaries. Absent any future, more specific federal regulation on this topic, it would be prudent to follow other applicable federal and state laws that provide certain protections for persons who are victims of PII theft. Those protections, as well as others available from such risk transfer vehicles as contractual risk shifting and insurance, should be taken into account when you address these network (privacy) risks in your organization. The potential loss of PII adds yet another dimension of complexity to the scenarios covered in this article and should be considered both in your preparation for, and your post-incident response to, network security breaches affecting your organization's retirement plans and other aspects of your operations.

Don't be a victim. Now is the time to be proactive in the management of these emerging network security risks.

© 2019 Andrew Robinson International Risk Management Consultants, Inc.