Fiduciary Responsibility

Data Breaches Highlight ERISA Legal Peril Attorney Says Plans May Some Day Face

Participant Privacy Concerns for Pension Plans

Key Focus: Pension plans could some day be liable under ERISA or state consumer protection law for failing to protect the private data of their participants.

Key Takeaway: Plans should adopt and apply best practices to protect this data and respond to any security breaches.

By David B. Brandolph

May 11 --Faced with the possibility of legal actions under an evolving prudence standard and state consumer protection laws, pension plans should be protecting the private data of their participants, attorneys told Bloomberg BNA in recent interviews.

Plans' responsibility to their participants regarding such personal information under the Employee Retirement Income Security Act has yet to be addressed by the courts or the Department of Labor, but Stephen P. Wilkes, of counsel with the Wagner Law Group in San Francisco, told Bloomberg BNA that "over time, at a minimum," he expects that plan sponsors and financial institutions that are fiduciaries will take various steps to protect private participant data and that such steps will become the "normal standard."

"Any deviation from that standard may arguably be a breach of duty to act prudently under ERISA," he said.

But while Wilkes suggests that a fiduciary standard under ERISA may be arising for plan sponsors, it doesn't appear that litigation in this area is on the radar of employee benefit plaintiff attorneys. Several contacted by Bloomberg BNA said the topic of pension plan responsibility under ERISA to protect private participant data is a topic they hadn't given much thought to.

Even if ERISA isn't yet fertile ground for potential lawsuits or sanctions, plan sponsors may be subject to liability from other sources. Plaintiffs' attorney Teresa Renaker, partner with Renaker Hasselman LLP in San Francisco, told Bloomberg BNA that "there's probably a more direct cause of action under consumer protection law and/or financial industry regulation. If a participant called me about a claim like this, I would most likely encourage them to speak to a consumer lawyer first."

Vulnerable Data.

Due to a number of recent high-profile attacks on corporate computer systems at Target Corp., Sony Pictures Entertainment and others, the public has become aware of how vulnerable their private information is.

In February, Anthem Inc. revealed that a cyberattack on its computer systems had resulted in the theft of names, addresses, telephone numbers, birth dates and Social Security numbers of some 80 million of the company's current and past customers, including health benefit plan participants of plan sponsors served by the insurer/plan administrator .

While the Anthem breach involved health plans, there are lessons that could be learned by pension plans. Like health plans, defined benefit and defined contribution plans have been expanding their use of technology to collect, analyze, share and store their participants' personal data. At the same time, the electronic transfer

of plan and participant financial information among plans, plan sponsors, participants and myriad plan service providers has also been increasing.

Is Private Participant Data Protected by ERISA?

Some questions to be answered to determine whether plans may be held responsible under ERISA or other laws for securing private participant data:

- Is private participant data a plan asset under ERISA's fiduciary duty provisions?
- Are plans required to protect private participant data as part of their duty under ERISA to act for the exclusive purpose of providing benefits to participants and their beneficiaries?
- Have plans breached their fiduciary duty of loyalty if a fiduciary's failure to protect private participant data caused participants' personal financial information to be compromised and they were able to show harm resulted?
- Will a standard of prudence develop under ERISA requiring specific steps for plans to take in protecting private participant data?
- Are plans required to protect private participant data under some state consumer protection law and/or financial industry regulation?

Question of Responsibility.

Consequently, there are questions as to the responsibility and potential liability of pension plans to protect their participants' private data in all the vehicles in which it is held and shared.

Wilkes said there are a "number of schools of thought" to answer questions of potential liability. Under one school, he said, plan sponsors would have a duty to protect private information about the plan and its participants from theft or intrusion, which could potentially result in the loss of plan assets or leave participants facing identity theft.

Under another school, Wilkes said, plan sponsors would be viewed as having enough responsibility and requirements to satisfy under ERISA and the tax code. Given that financial firms and other players in the retirement space, including the companies that sponsor pension plans, already have the legal responsibility to protect private data under various federal and state laws, Wilkes said some might ask whether it makes sense for sponsors or fiduciaries to be burdened with yet another set of rules, presumably issued by the Labor Department, that may discourage companies from having a retirement plan at all.

DOL Input.

Wilkes said the Labor Department will likely bring "focus to this question," although not before it completes the process for its current fiduciary definition proposal. The ERISA Advisory Council is slated to discuss the topic of privacy at its May 29 meeting .

When it acts, the Labor Department may decide that it wants to adopt privacy rules similar to what the Department of Health and Human Services requires for patient information under the Health Insurance Portability and Accountability Act, and impose such rules as a fiduciary obligation, Wilkes said. It also may decide whether participant data is a plan asset subject to ERISA fiduciary protection, he said.

Alternatively, Wilkes said the Labor Department may want to let the existing patchwork of nonintegrated federal and state law be the primary regulatory force. If so, the DOL may want to advise plans and participants on what is at stake with their personal data, he said.

There are some interesting legal theories both in support of and against the idea that private participant data is a plan asset subject to fiduciary protection under ERISA, Wilkes said. He added that a decision that such data is subject to such protection would be a "huge DOL policy decision or congressional legislative decision."

Plaintiffs' counsel Renaker, addressing whether ERISA would apply to private data breach actions filed by participants, said that a case could probably be made for a "breach of the fiduciary duty of loyalty if a fiduciary's actions caused participants' personal financial information to be compromised and they suffered harm as a result." She said, though, that it "could be tricky to identify an equitable remedy that would provide relief to the participants."

As an example of the idea that sponsors and fiduciaries will, at least over time, take steps to protect participant data, Wilkes said that, if in the future it becomes part of the normal standard for plan sponsors or registered investment advisers to encrypt their data when transmitting it, "someone will eventually raise the argument that the failure to do so is imprudent."

List of Best Practices.

Wilkes provided what he described as a "not all inclusive" list of best practices for plan fiduciaries to follow in protecting the private data of plan participants:

- Limit account access to key personnel.
- Use proven software from a "whitelist" of proven vendors, while avoiding software known for problems from a "blacklist."
- Use best-in-class software to protect against virus and e-mail intrusions, including the protection and filtering of all access to the plan or provider website.
- Have timely and automatic updates of all software.
- Operate on only industry-approved and -vetted operating systems, including on all laptops, smartphones and other remote devices.
- Back up data on a secure storage facility.
- Have written policies and procedures that are in full compliance with applicable state and federal law.
- Perform due diligence on all third-party vendors that will have access to plan data, and obtain appropriate representations and warranties in service agreements.
- Identify a person, such as a chief privacy officer, to be responsible within the organization for privacy and data security issues. In smaller companies, be sure to include such responsibilities in the job description of an identified and accountable person.

By David B. Brandolph

To contact the reporter on this story: David Brandolph in Washington at dbrandol@bna.com

To contact the editor responsible for this story: Jo-el J. Meyer at jmeyer@bna.com