ERISA's impact on data breach lawsuits

April 07, 2016 | from HR.BLR.com

By Sandra R. Mihok

Health insurance companies have increasingly become the target of cyberattacks, a trend which has spurred a wave of class action lawsuits brought by individuals whose personal information has been breached.

Typically, the lawsuits allege violations of various state laws and seek recoupment of a portion of premiums which they claim was paid to the insurer to keep their personal information secure. When the class action involves employer-sponsored group health plans, these state law claims might be preempted by Employee Retirement Income Security Act (ERISA), which contains specific enforcement mechanisms.

The U.S. District Court for the Northern District of California has recently found that such state laws are preempted by ERISA. If preemption applies, and plaintiff lawyers attempt to pursue such claims under ERISA, employers will want to pay particular attention to plan documents and Health Insurance Portability and Accountability Act (HIPAA) security procedures.

U.S. District Court for the Northern District of California rules for 2nd time on ERISA

The District Court in California has ruled, for the second time, that ERISA preempts state law contracts and related claims in data breach lawsuits involving Anthem Blue Cross and Blue Shield's data breach that occurred in February of 2015. *(Smilow v. Anthem Life& Disability Ins. Co. (In re Anthem, Inc. Data Breach Litig.),* N.D. Cal., No. 5:15-cv-04739-LHK, 11/24/15).

This class action was originally filed in New York state court on behalf of all New York citizens insured by Anthem whose protected health information had been compromised in the February 2015 cyberattack.

The participants alleged negligence, breach of implied contract, unjust enrichment, and invasion of privacy, among other state law claims. The plaintiffs argued that a portion of the premium paid to Anthem should have been spent on reasonable data security, and therefore they were entitled to the difference between the premiums actually paid and the actual value of the services they received. As part of multidistrict litigation, the case was moved to the Northern District of California.

Anthem removed the case to federal court, arguing that the state law claims were preempted by ERISA. The plaintiffs requested that the court remand the case to state court.

The court applied a two-part test of ERISA preemption set forth in the Supreme Court decision *Aetna Health, Inc. v. Davila*, 542 U.S. 200 (2004). The test provides that a state law cause of action is completely preempted if (1) an individual could have brought the claim under ERISA Section 502(a)(1)(B) as a claim for benefits; and (2) no other independent legal duty is implicated by the defendant's actions.

The court found that both parts of the test were met. Participants claims were premised on the insurance contract which was part of an ERISA plan, and therefore, they could have brought their actions under Section 502(a).

In addition, the court determined that Anthem did not have an independent legal duty to protect participants' privacy pursuant to state law because the obligation to protect privacy under state laws wouldn't exist if the plan didn't exist.

Further, the handbook describing the plan benefits included a statement that state privacy laws that are more stringent than HIPAA would apply, and therefore the court determined that Anthem's duty to comply with state privacy laws arose under the ERISA plan.

What are the implications of the Court's decision?

HIPAA requires plan sponsors to amend their plan documents in order to establish permitted uses and disclosures of protected health information and protect the privacy and security of such information. In addition, participants are provided with notices of privacy practice, and often the notice is incorporated into the plan's summary description. Thus, ERISA can be an enforcement mechanism creating a private right of action in favor of plan participants.

A civil action may be brought "(1) by a participant or beneficiary … (B) to recover benefits due to him under the terms of his plan, to enforce his rights under the terms of the plan, or to clarify his rights to future benefits under the terms of the plan." 29 U.S.C. § 1132(a)(1)(B).

Uncertainties exist as to how a participant might be able to succeed under ERISA 502(a)(1)(B) to make a claim based on a cyberattack. For example, the participant must be able to point to plan language to make a claim that the benefit is provided by the plan, either expressly or impliedly.

While plan documents that are amended for HIPAA contain provisions regarding the plan's establishment of reasonable security measures, most plans do not provide any specific enumerated plan benefit for cyberattacks. Therefore, participants will likely be required to show that this is an implied benefit, but it will be difficult to quantify the portion of participant premiums that are attributable to security measures, especially when the employer subsidizes a substantial portion of the plan benefits.

Also, employers may be able to add language to plan documents which expressly provide that the plan does not provide benefits or refund premiums for cyberattacks. Further, to complicate matters for participants and class action attorneys, participants generally must exhaust their administrative remedies, i.e. the plan's claims and appeals procedures, prior to filing any lawsuit.

If ERISA applies, participants would also be able to bring claims for breach of fiduciary duty. Cyberattacks are typically aimed at health insurers or third party administrators, but in order to make a claim against an insurer or third party administrator, a participant must allege that the party was a plan fiduciary.

Generally, under ERISA, an insurer or third party administrator's fiduciary functions relate to deciding claims and appeals under the plan, but not to the other ministerial or administrative services that are provided. On the other hand, the plan documents typically name the plan sponsor or a plan committee as the named fiduciary.

Thus, employers may be named as defendants in these lawsuits if it helps make out an ERISA claim. In this context, a participant must allege that the employer breached a duty of loyalty or care owed to the plan by not taking adequate steps to secure plan data, or by not monitoring the actions of the insurer or third party administrator.

The employer may be able to defend such claims if it took all actions necessary to comply with HIPAA, including entering into business associate agreements when required. Participants may need to argue that a prudent fiduciary would have taken additional measures.

Notwithstanding the *Smilow* decision, the state of the law on ERISA preemption of data breach suits is far from settled. For example, the court's ruling in *Smilow* is contrary to the decisions of other courts, including other district courts in California., (*See eg. Wickens v. BlueCross of California d/b/a Anthem*, 2015 WL 4255129 (S.D. Ca. July 15, 2015); *Rose v. HealthComp* (2015 WL 4730173 (E.D. Ca. August 10, 2015).

Nonetheless, the decision sets the stage for an argument in favor of ERISA preemption which in certain cases may benefit insurers, administrators, and employers faced with state law challenges.