Privacy Risks for Retirement and Other Non-Health Benefit Plans

A Lexis Practice Advisor® Practice Note by
John L. Utz, Utz & Lattan, LLC


John L. Utz

This practice note discusses the litigation risks faced by sponsors of employee benefit plans other than health plans regarding their handling of personally identifiable information (PII) on behalf of plan participants and beneficiaries. The note focuses on retirement plans under the Employee Retirement Income Security Act (ERISA), but also addresses employee welfare plans not required to comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

The note focuses on:

- ERISA Requirements for Personally Identifiable Information
- Participant Claims against Fiduciaries and Plan Sponsors for Data Breaches
- Actions to Mitigate Privacy Risk

For a discussion of the HIPAA rules on protected health information, see HIPAA Privacy, Security, Breach Notification, and Other Administrative Simplification Rules. For related practice notes on data privacy issues, see Privacy and Data Security Considerations When Negotiating or Reviewing a Transaction or Agreement and Privacy Policies: Drafting a Policy.

ERISA REQUIREMENTS FOR PERSONALLY IDENTIFIABLE INFORMATION

ERISA requires plan fiduciaries to act with the "care, skill, prudence, and diligence under the circumstances then prevailing that a prudent man acting in a like capacity and familiar with such matters would use." ERISA § 404(a)(1)(B) (29 U.S.C. § 1104(a)(1)(B)). Although the statute does not explicitly require fiduciaries to protect participants' PII, one can imagine participants someday arguing that ERISA's prudence requirement imposes an obligation to protect their privacy. To date, courts have done little in the way of imposing a fiduciary obligation to try to protect participants' privacy outside the obligations imposed by HIPAA.

When applying ERISA's prudence requirement, courts and the Department of Labor (DOL) generally focus on whether the fiduciary followed a good process. Courts and the DOL focus less on the result and more on the diligence in considering and addressing concerns. As the processes for reducing risk security and privacy rules become better developed and more commonly used by businesses, governments, and individuals, one can expect that what is prudent in handling PII will change accordingly.

For a discussion about ERISA's fiduciary rules, see Fundamentals of ERISA Fiduciary Duties.

Personally Identifiable Information

HIPAA defines protected health information (PHI) for plans subject to that statute. See 45 C.F.R. § 160.103. For plans not subject to HIPAA, plan fiduciaries may look elsewhere for a working definition of PII. One definition of PII comes from the Office of Management and Budget (OMB):

> [I]nformation which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

Office of Management and Budget Memorandum M-07-16 "Safeguarding Against and Responding to the Breach of Personally Identifiable Information."

PII typically includes other information that is linked to the individual, such as:

- Email addresses
- Credit card information
- Bank account information

Notable Security Breaches

While courts do not yet seem to hold fiduciaries to a high standard regarding data privacy, what is prudent inevitably changes with time. As security breaches become increasingly routine, and therefore more a part of the consciousness of the public—and, perhaps more important, the consciousness of judges—the standards for prudent protection of PII may become stricter.

While the increased frequency and severity of security breaches may lead to a heightened obligation to protect PII, it could also reasonably lead fiduciaries to conclude that it will be virtually impossible to assure that no security breach will occur or that PII will not be misused. The National Security Agency (NSA), which describes itself as "the world leader in cryptology" has itself been hacked. That breach not only suggests that benefit plan fiduciaries cannot assure complete data security, the hacking tools stolen from the NSA may actually increase the threat to benefit plans.

Besides the NSA breach:

- A hack of the Central Intelligence Agency (CIA) in 2017 exposed both secret documents and the CIA's own hacking tools.
- A breach of the Securities Exchange Commission's (SEC's) computer system in 2016 exposed that PII was hacked in 2016.

Security breaches have extended to private entities as well, including:

- Yahoo (affecting the information of all 3 billion of its customers)
- Deloitte and J.P. Morgan Chase & Co. (which compromised the accounts of 76 million households and 7 million small businesses) –and–
- Equifax Inc. (which may have exposed sensitive information of over 140 million Americans, including PII)

The Deloitte hack compromised a server that contained emails from clients including not only some of the world's largest multinational businesses, but also the United Nations and the U.S. Departments of State, Energy, Homeland Security, and Defense. The Equifax hack affected nearly 40% of the U.S. population.

PARTICIPANT CLAIMS AGAINST FIDUCIARIES AND PLAN SPONSORS FOR DATA BREACHES

ERISA does not explicitly require plan fiduciaries to take special action to protect PII. But ERISA requires fiduciaries to act with the "care, skill, prudence, and diligence under the circumstances then prevailing that a prudent man acting in a like capacity and familiar with such matters would use." ERISA § 404(a)(1)(B) (29 U.S.C. § 1104(a)(1)(B)). Besides arguing that a privacy breach was a consequence of a fiduciary's failure to meet this standard, there are many state law claims a participant might assert if a privacy breach occurs, as described below in the section titled "Participant State Law Claims."

Is There an Injury-in-Fact?

Given the breaches described earlier, fiduciaries and plan sponsors might reasonably wonder whether there is any point in trying to improve plan data security. And, relatedly, they might question whether participants or others seeking to hold fiduciaries liable can argue that the fiduciaries' actions or failure to act were the proximate cause of any participant injury. A fiduciary might argue that any injury claimed by a participant whose PII was compromised was just as likely to have resulted from some other (non-ERISA plan) breach of his or her information.

A fiduciary defendant might argue that, absent a participant's ability to identify a trail from the breach of plan information to the harm the participant suffered, the participant can't establish that he or she suffered an injury as required to sue. The argument would be that to sue in federal court the participant must have an injury-in-fact within the meaning of Article III of the Constitution, and must also have suffered an injury to have recourse under ERISA. See, e.g., Lee v. Verizon Communications, Inc., 837 F.3d 523 (5th Cir. 2016); Thole v. U.S. Bank, N.A., 873 F.3d 617 (8th Cir. 2017). And even if state claims may proceed in state court—for example, where complete preemption is inapplicable and state law claims are similarly not preempted by ERISA—it may be difficult to demonstrate losses or damages on which a participant could collect.

However, at least one court has rejected the defense that the ubiquity of security breaches precludes plan participants from establishing they have been harmed by a plan-related breach. Specifically, in *In re Anthem, Inc. Data Breach Litigation,* the court considered defendants' argument that the plaintiffs had not sufficiently pleaded damages for loss of value of PII. 2016 U.S. Dist. LEXIS 70594 (N.D. Cal. 2016). A 2015 cyberattack on Anthem's databases resulted in the theft of information relating to about 79 million people. The information taken may have included names, dates of birth, social security numbers, health care ID numbers, home addresses, email addresses, and employment information, including employment data. While this note focuses on risks to non-health plans, and the *Anthem* case involves a health plan, the legal analysis as to whether a participant is damaged by a privacy breach should generally be the same regarding all types of benefit plans. For reference to the settlement terms of the *In re Anthem, Inc. Data Breach Litigation case,* see FAQs, Anthem Data Breach.

Prior to the *Anthem* case settling in 2017, the district court addressed whether participants had adequately pleaded that they had been damaged. The court concluded that the plaintiffs had sufficiently pleaded damages, citing Ninth Circuit case law in which plaintiffs sufficiently pleaded economic injury by claiming "that the[ir] PII was stolen and posted on file-sharing websites for identity thieves to download." Corona v. Sony Pictures Entertainment, Inc., 2015 U.S. Dist. LEXIS 85865 (C.D. Cal. 2015).

The *Anthem* court rejected defendants' argument that plaintiffs plead both that there was a market for their PII and that they somehow also intended to sell their own PII. Instead, the court said, plaintiffs can meet their pleading requirement by alleging there was either an economic market for their PII or that it would be harder to sell their own PII, but need not plead both. But, even if both requirements applied, the court said the plaintiffs' complaint would have been adequate. That is because the complaint asserted that the plaintiffs' PII "is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the cyber black-market for years." 2016 U.S. Dist. LEXIS 70594 at 130.

Article III Standing

One court rejected privacy claims based on the theft of private information because the claims failed to establish standing under Article III of the U.S. Constitution. To have Article III standing, the threat must be imminent, which means it must not be "too speculative" and must be "certainly impending." E.g., Curry v. Regents of the Univ., 167 F.3d 420 (8th Cir. 1999). Although in a non-ERISA case, the District Court for the Western District of Missouri found an individual's claims on the risk of future identity theft too speculative to afford Article III standing. Cox v. Valley Hope Ass'n., 2016 U.S. DIST. Lexis 119663 (W.D. Mo. 2016). There, the court addressed privacy claims relating to the theft of a laptop computer owned by a drug and alcohol treatment center. The laptop contained private treatment and identification information for over 50,000 patients. The laptop was secured with a password, but the information stored on the device was not encrypted. The treatment center sent letters to patients informing them of the theft. In a putative class action, the plaintiff argued that he had "suffered damages, including and without limitation, loss of privacy, confidentiality, embarrassment, humiliation, loss of income, [and] loss of enjoyment of life." Id. n.1. But the plaintiff offered little more by way of explanation, and no facts suggesting that his privacy was actually invaded, that he actually suffered embarrassment or humiliation, or that he spent any monies because of the laptop theft. The alleged injuries were, therefore, conclusory, and as a consequence, inadequate.

For further discussion of standing in ERISA actions, see The Law of Life and Health Insurance § 1A.04, paragraph [4].

Participant State Law Claims

The risk to retirement and other non-health plan fiduciaries (that is, to fiduciaries of plans not subject to HIPAA) is not just the concern about ERISA's fiduciary duty of prudence. There are also a multitude of state law causes of action that could bite fiduciaries. Each of the 50 states has a privacy law. But most are not comprehensive in scope. Every state imposes notification requirements if a security breach occurs. The District of Columbia, Guam, Puerto Rico, and the Virgin Islands also have some form of notice requirement. Most of these breach notification laws, however, are enforced by the state attorney general and do not provide for a private right of action. For a state-by-state chart detailing state data breach notification laws, see Data Breach Notification Enforcement and Penalties State Laws Chart.

At least 32 states and Puerto Rico have laws requiring that PII be destroyed, disposed of, or otherwise made unreadable or undecipherable, once the PII is no longer to be retained. Of concern greater than the breach notification and data disposal statutes, at least 13 states impose requirements for the maintenance of reasonable security procedures and practices in connection with personal information for the state's residents. And several states have legislation restricting the use of social security numbers, which are still utilized in the administration of some retirement plans.

Perhaps more concerning than the state statutes noted above are state common law causes of action, such as state privacy, negligence, implied contract (to keep information private and secure), covenant of good faith and fair dealing, and unjust enrichment common law claims. Also of concern are potential claims under broad state unfair or deceptive business practices acts.

Preemption of State Law Claims

While ERISA frequently preempts state law claims, the modest case law on privacy breaches and PII matters is split on preemption. The preemption argument is strongest where the security breach or misuse of private information occurs in a function central to the administration of a benefit plan.

- **ERISA preemption**. The Sixth Circuit appears to have been the first circuit to take up this question, although its decision seems to be in the minority. In re General Motors Corp., 3 F.3d 980 (6th Cir. 1993). There, the Sixth Circuit held that ERISA preempted state law claims relating to a failure to keep employee assistance plan information confidential. The court's sparse analysis noted that the claims were preempted even though the plaintiff did not seek to be made whole by receiving an award of the type of benefit the employee assistance program was designed to provide. The plaintiff was asking for something different (or more) than benefits under the plan, yet the claims were still preempted.
- **No ERISA preemption**. In cases decided by the Fourth and Ninth Circuits, by contrast, participant state law claims were not preempted by ERISA where the complaints concerned activity that was not core to the administration of a benefit plan.
    - In *Darcangelo v. Verizon Communications., Inc.*, the Fourth Circuit refused to dismiss on ERISA preemption grounds certain state law claims brought by a disability benefit plan participant against her employer and the administrator of the disability plan. 292 F.3d 181 (4th Cir. 2002). In doing so, the court concluded that the key question was whether the administrator obtained the plaintiff's medical information either while processing the plaintiff's benefits claim or while performing any of its administrative duties under the plan. If so, the Fourth Circuit said, ERISA would preempt the state law claims. But if instead the administrator was not performing any of its duties as plan administrator, but obtained the information solely to assist the employer in establishing that the plaintiff threatened her coworkers, the state law claims would not be preempted.
    - In *Dishman v. UNUM Life Ins. Co. of America*, the Ninth Circuit held that ERISA did not preempt a state law claim even though the claim had a relationship to plan administration. 269 F.3d 974 (9th Cir. 2001). In so holding, the court quoted the Supreme Court, saying ERISA preemption does not occur "if the state law has only a tenuous, remote, or peripheral connection with covered plans, as is the case with many laws of general applicability." 269 F.3d at 984 (quoting New York Conference of Blue Cross & Blue Shield Plans v. Travelers Insurance Co., 514 U.S. 645, 661 (1995)). That the complained-of conduct in *Dishman* allegedly occurred during the insurer's administration of a plan did not create a relationship sufficient to warrant preemption. The Ninth Circuit was "certain that the objective of Congress in crafting [ERISA preemption provision] was not to provide ERISA administrators with blanket immunity from garden variety torts which only peripherally impact daily plan administration."

"Reference to" versus "Connection with" State Law Analyses

In the *Anthem* case noted earlier, the court held that California contract law claims were not preempted. 2016 U.S. Dist. Lexis 70594. In its preemption analysis for the breach of contract claim, the district court looked to the Supreme Court's decision in *Gobeille v. Liberty Mutual Insurance Co.,* where the Supreme Court noted:

> [The Supreme Court's] case law to date has described two categories of state laws that ERISA [expressly] pre-empts. First, ERISA pre-empts a state law that has a "reference to" ERISA plans. To be more precise, where a State's law acts immediately and exclusively upon ERISA plans or where the existence of ERISA plans is essential to the law's operation, that "reference" will result in pre-emption. Second, ERISA pre-empts a state law that has an impermissible "connection with" ERISA plans, meaning a state law that governs a central matter of plan administration or interferes with nationally uniform plan administration.

136 S. Ct. 936, 943 (2016) (Internal quotation marks and ellipses omitted).

In the quote above, the Supreme Court described two types of preempted state laws. One has a "reference to" ERISA plans. The second has a "connection with" ERISA plans. As to the "reference to" category of preempted states laws, neither the plaintiffs' California contract law claims, nor their New York unjust enrichment law claims or New York deceptive business practice claims involved state laws that "act[ed] exclusively upon ERISA plans," nor was "the existence of ERISA plans . . . essential to [those state laws'] operation." Gobeille, 136 S. Ct. at 942. Instead, they were "laws of general application, and [did] not focus exclusively (or, for that matter, even primarily) on ERISA plan administration." As such, they were not preempted by reason of a "reference to" ERISA plans.

As to the "connection with" category of preempted laws, the district court in *Anthem* said the analysis was tougher, but the state breach of contract, unjust enrichment, and deceptive business practices claims nonetheless did not have a "connection with" ERISA plans. In contrast to the claims under consideration by the court—which related to data privacy, not benefit payments—ERISA preempts state laws having a connection with ERISA plans by "mandat[ing] employee benefit structures or their administration." 2016 U.S. Dist. Lexis 70594, at *235 (citing *Travelers* and *Dishman*). So, for example, if a "statute governs the payment of benefits, a central matter of plan administration," it will be preempted. Explaining the types of laws having a connection with ERISA plans, the court quoted from the Second Circuit's decision in Gerosa v. Savasta & Co., 329 F.3d 317 (2d Cir. 2003), saying "state laws that . . . tend to control or supersede central ERISA functions—such as state laws affecting the determination of eligibility for benefits, amounts of benefits, or means of securing unpaid benefits—have typically been found to be preempted." 2016 U.S. Dist. Lexis 70594, at *236.

The conclusion the district court took from the preemption case law is that "laws that implicate the administration of ERISA benefits are subject to express preemption, and laws that do not are not preempted." Id. Because the court concluded that the *Anthem* claims were not for ERISA benefits, but were instead claims relating to data privacy, those claims did not implicate ERISA benefits. So, the claims did not relate to the administration of benefits. As the court put it, there is no suggestion in ERISA that "protecting customer PII should be considered an ERISA benefit." 2016 U.S. Dist. Lexis 70594, at 229. Benefits, in the health plan context, instead concern payments for healthcare-related services. The court found support for this conclusion in *Wurtz v. Rawlings Co.,* where the Second Circuit held that tort damages a plaintiff suffered in an automobile accident, which might overlap or supplement medical benefits the plaintiff received, should not be considered benefits for purposes of ERISA. 761 F.3d 232 (2d Cir. 2014). In *Anthem*, the plaintiffs did not make a claim for the payment of medical or healthcare expenses. They instead alleged that the defendants violated certain privacy obligations, "a legal area where ERISA is silent."

The court preceded its preemption analysis with the assertion that "no circuit court has ever applied ERISA preemption—express or complete—to preclude a plaintiff from moving forward with state law claims arising out of a data breach." Therefore, the defendants were asking the court to "break new ground" to find that the general "presumption against preemption" is overcome in a field where it has never been applied. The court declined, and did not dismiss the state law claims as preempted. 2016 U.S. Dist. Lexis 70594, at *227.

Additional ERISA Preemption Case

If the court in *Anthem* is right, the preemption question becomes one of whether the laws implicate the administration of benefit plans. Clever pleading should not, however, save a claim that should, in fact, preempted. For example, in Hogan v. Jacobson, 823 F.3d 872 (6th Cir. 2016), where the Sixth Circuit held that a disability benefit plan participant's negligence per se claim against nurses—relating to the nurses' processing of a benefit claim—was preempted. It was preempted even though it was plead as a state law negligence claim related to the nurses' activities. That is because the claim was, in reality, a claim for ERISA benefits. The alleged negligence related to the negligent processing and denial of the participant's disability benefit claim, which arose solely from a plan subject to ERISA. The court contrasted the plaintiff's claims with those where there is a "truly independent state law tort claim" brought between parties that "happen also to have an ERISA-based relationship." The Sixth Circuit cited as examples of the latter both *Darcangelo* and *Dishman* above.

In *In re Premera Blue Cross Customer Data Security Breach Litigation*, the court held that state statutory and common law claims were not preempted by ERISA. 2017 U.S. Dist. LEXIS 18322 (D. Or. 2017). Although this was the same result as in *Anthem*, the court diverged from the *Anthem* court's analysis. Looking in part to the Ninth Circuit's decision in *Dishman*, the court found that "although there is some relationship between data security and the administration of Plaintiffs' ERISA plans, it is not enough to overcome the presumption against preemption of state law." 2017 U.S. Dist. LEXIS 18322, at *66. Here, the plaintiffs had sufficiently alleged an "independent legal duty separate from the ERISA plan" implicated by the defendant's alleged action. Consequently, complete preemption did not apply. And although this conclusion that complete preemption did not apply seems to beg the question before the court— whether the state law claims were preempted—he court summed up with language that may point to a fair rule of thumb, redolent of the Supreme Court's old *Mackey* decision. See Mackey v. Lanier Collection Agency & Serv., 486 U.S. 825 (1988). The court said the "state statutory and common law claims here are generally applicable, and they function irrespective of the existence of an ERISA plan." As a consequence, the state law causes of action did not relate to the "essence of the [ERISA] plan itself," and therefore were not preempted.

Relying on *Dishman*, a court held that invasion of privacy claims relating to an investigation under a long-term disability plan were not preempted. Vaught v. Hartford Life & Accident Ins. Co., 2011 U.S. Dist. LEXIS 98945 (S.D. Ohio 2011). In *Vaught*, the plaintiff was a participant in a long-term disability plan. She alleged that in investigating whether her disability benefits should be terminated, the insurer violated and invaded her privacy by videotaping her while she was on her own property and while in her vehicle. The court found that the plaintiff's claim for invasion of privacy should not be dismissed on preemption grounds. Although the court found it a close question whether the plaintiff's invasion of privacy claim was so connected to a denial of ERISA benefits as to be preempted, the court said the alleged conduct might be beyond the bounds of a reasonable investigation and that "tortious conduct that amounts to an invasion of privacy would not 'relate to' the administration of the plan for purposes of preemption."

Complete Preemption versus Preemption

Notably, the court in *Premera* seemed to be asked to address preemption, but in doing so moved back and forth between references to complete preemption and preemption, conflating the two concepts. Complete preemption is a jurisdictional concept relating to whether claims made in state court—and ostensibly about state law causes of action—may be removed by a defendant to federal court because ERISA wholly displaces one or more of the state law causes of action. As the Supreme Court has put it, "any state-law cause of action that duplicates, supplements, or supplants the ERISA civil enforcement remedy conflicts with the clear congressional intent to make the ERISA remedy exclusive and is therefore pre-empted." Aetna Health Inc. v. Davila, 542 U.S. 200, 209 (2004). In a stronger statement, the court added, "ERISA civil enforcement mechanism is one of those provisions

with such 'extraordinary pre-emptive power' that it 'converts an ordinary state common law complaint into one stating a federal claim for purposes of the well-pleaded complaint rule.'" As a consequence, "causes of action within the scope of the civil enforcement provisions of [ERISA] § 502(a) [are] removable to federal court."

State law claims can be preempted without the defendant having a right under the complete preemption doctrine to remove a state court action to federal court. It is unnecessary for a claim to be completely preempted for it to be preempted. Where the issue is only whether a state law cause of action is preempted, and not the jurisdictional question involving complete preemption, the proper question is whether the state law "relates to" ERISA plans. In the discussion of *Anthem* above, a state law will generally relate to ERISA plans if the state law either has an impermissible "connection with" ERISA plans (generally because it either involves a central matter of plan administration or it interferes with nationally uniform plan administration) or the law makes "reference to" ERISA plans.

The reason some federal district courts, when attempting to address ERISA preemption, seem to lean on complete preemption cases might be they assume if claims are completely preempted they are, *a fortiori*, also preempted. This is sort of true. Complete preemption probably implies preemption, or something similar—the "something similar" because the state law claim is transformed into a federal claim. One way or another the state law claim is not going forward. Put differently, where there is complete preemption under the Supreme Court's framework in *Davila*, either the state law claim is transformed into a federal claim or it is preempted, whether or not that preemption occurs under ERISA. Here's how the Supreme Court put it in *Davila*, after reminding that removal is appropriate on complete preemption grounds, if both:

- The plaintiff could have brought the claim under ERISA Section 502(a)(1)(B) (29 U.S.C. § 1132(a)(1)(B)).
- No other independent legal duty is implicated by the defendant's actions:

  A state cause of action that provides an alternate remedy to those provided by the ERISA civil enforcement mechanism conflicts with Congress' clear intent to make the ERISA mechanism exclusive., and therefore would be preempted [:] . . . "[e]ven if there no express preemption [under ERISA Section 514(a)]." (Quoting Ingersoll-Rand Co. v. McClendon, 489 U.S. 133, 142 (1990)). 542 U.S. n.4.

So, complete preemption means the claims are preempted somehow. The frustrating point is that claims can be preempted without there being complete preemption, yet district courts are often not punctilious in keeping the two concepts straight. A court presented with a preemption question (and not whether it was proper to remove the case from state to federal court on complete preemption grounds) should be focused on preemption cases, not complete preemption cases.

For a further discussion on preemption, see ERISA Preemption and The Law of Life and Health Insurance § 1A.02.

ACTIONS TO MITIGATE PRIVACY RISK

Fiduciary Prudence

Fiduciary prudence is about process. Even though ERISA does not specifically require it, it may be wise for plan fiduciaries to start considering, and addressing, privacy and security concerns as they relate to retirement, disability, and other plans not subject to HIPAA standards. While no foolproof processes can be implemented, as a matter of procedural prudence it may be time to start what may be an interminable and tedious process of considering, and continually improving, plan security and protecting private information.

Fiduciaries can take a few basic, and not especially painful, steps to start. These steps may be adequate for the time being, at least in satisfying fiduciary's ERISA prudence obligations.

Security and Privacy Processes

The most important step may be to focus on the security and privacy of information in the hands of plan vendors. Retirement plan recordkeepers, trustees, and other financial institutions are typically a greater target for those seeking access to confidential information than is any one employer or other plan sponsor. That is because plan vendors hold data for lots of plans (and other, non-plan clients). That data will often include information that could lead to the theft of plan participants' identities, such as where a retirement plan vendor associates names with social security numbers.

Stolen participant information was reportedly used in June 2016 to take $2.6 million in unapproved loans from the Chicago Deferred Compensation Plan, a large, $3.6 billion, Section 457(b) plan. The loans were taken from 58 participant accounts, but the recordkeeper reportedly restored the filched monies within five days.

The compromise of a retirement plan recordkeeper's system could lead to unauthorized benefit payments, such as withdrawals from 401(k) accounts. If fiduciaries follow a proper and properly disclosed process, those fiduciaries may be shielded from liability arising from a data breach.

Foster v. PPG Industries illustrates this point. 693 F.3d 1226 (10th Cir. 2012). In *Foster*, a former employee lost all the monies in his 401(k) account when his ex-wife misappropriated them after the participant moved away from the address he left on record with the 401(k) plan. The participant sued his former employer and the 401(k) plan to recover the monies stolen from his account. The court did not require the plan administrator to reimburse the participant for the amount the ex-wife improperly took, reasoning that the plan administrator properly disclosed to participants the plan's procedures for requesting distributions electronically and closely followed those procedures.

Those procedures included:

- An automated system enabling participants to access accounts online
- Notifying participants about how to use the system –and–
- Notifying participants about upcoming enhanced security measures, which included using unique user IDs, rather than social security numbers, and more complex password requirements

Even with a well-designed process, though, failures can occur. The plaintiff in *Foster* had his account compromised due to the plan sending mail to the participant's former residence, as the participant never notified the plan sponsor of his change of address. This allowed the ex-spouse to use the enhanced security measures to gain unauthorized access to the account and wipe out the assets in the account.

Unauthorized Access to Plan Data

Bad actors have posed a risk to benefit plans for some time. The American Institute of Certified Public Accountants (AICPA) reported to the DOL's Advisory Council on Employee Welfare and Pension Benefit Plans that, by 2011, data breaches had occurred in pension plans from:

- Unauthorized user hacking into the plan administrative system after gaining administrative privileges to the accounts and changing account information followed by a fraudulent distribution of funds from the participants' accounts to the unauthorized user

  - The hacker gained access to the system by planting a virus on the company's computer. It is believed the virus enabled the hacker to capture keystrokes when made by an authorized person, enabling the hacker to capture login information and passwords of the plan participants.
- Unauthorized person logging into broker website, entering ID and password, and securing payment sent to a name different from the name on the account
- Person hacking into database to gain access to over 500,000 participants' PII due to failure of the plan (and administrators) to install security system updates
- Email hoax (phishing attack) that directed participants to a look-alike website prompting participants to share personal data including Social Security numbers (SSNs)
- Employee downloading confidential information for over 450,000 participants to a home computer
- Several examples related to the ease with which PII was fraudulently obtained from laptops
- Multiple examples involving SSNs on printed communications that were, often, either mailed to wrong addresses or the information was made visible to others
- Employee stealing electronic tapes that contained PII of plan participants and/or beneficiaries
- Auditors who received CDs with PII of participants and beneficiaries in benefit plans they did not currently audit –and–
- Payroll provider using the same password for all clients when the payroll system was established

ERISA Advisory Council, Privacy and Security Issues Affecting Employee Benefit Plans, (Nov. 2011).

Ransomware

The cybersecurity risks for benefit plans do not relate solely to the potential for the theft of participants' identities or fraudulent benefit payments. There is also the risk of a ransomware attack, with the attendant possibility of crippling plan administration. For example, a security breach at a plan reportedly occurred when a hacker gained control of one of the union's computer servers. The hacker demanded three Bitcoins to restore access to records relating to the plan, which reportedly held over $500 million in assets. The ransom was apparently not paid, and a backup server allowed the plan to continue operations.

Improving Data Security Processes

To improve data security processes, plan fiduciaries may wish to start with the plan's vendors. Plan fiduciaries may find it easier to take meaningful steps with vendors than to reshape the internal information technology processes at the plan sponsor. For most single employer plans benefit plan data is handled through a human resources or employee benefits department merely a part of the larger employer. That HR (or benefits) department will often not have a separate information technology system, nor a dedicated information technology staff. Instead, its ability to effect IT changes helpful from a security and privacy perspective will turn on the HR/benefits department's ability to convince the employer either to change its company-wide system or to devote IT resources to the creation and maintenance of special systems within the HR or benefits function. Given the scarceness of IT resources at most employers, this may prove a tall order. It doesn't mean one doesn't try, when appropriate, to implement system changes internally that will help protect the privacy and security of benefit plan information, but the low-hanging fruit may instead lie in vendor relationships. Although we know from experience in complying with HIPAA there are non-IT driven steps one can take to improve privacy practices, the ability of a benefits department to improve IT security itself will typically depend on the cooperation and availability of other resources at the employer (or other plan sponsor).

Requests for Proposals

In requests for proposal (RFPs), fiduciaries may wish to inquire about the privacy and security standards vendors have in place. Fiduciaries may wish to ask for copies of AICPA System and Organization Control (SOC) Reports. A precursor of these reports were the SAS 70 reports. For a checklist on implementing RFPs for ERISA plan services, see Request for Proposal Checklist (Retirement Plan Service Provider).

System and Organization Controls (SOC) Reports

There are three types of SOC reports: SOC 1, SOC 2, and SOC 3. Customers of service organizations, such as fiduciaries and plan sponsors of benefit plans, can use SOC reports to help evaluate the effect on the vendor's financial statements of controls that the vendor has in place. One may wonder why statements about the effect of controls on the vendor's financial statements would be of value to plan fiduciaries. The answer is that two of the three types of SOC reports—SOC 2 and SOC 3 reports—address cybersecurity controls at the vendor level. These are relevant to:

- The security, availability, and processing integrity of the systems the vendor uses to process customers' data –and–
- The confidentiality and privacy of the information processed by these systems

SOC for Service Organizations: Information for Service Organizations, AICPA.

SOC 2 reports. There are two types of SOC 2 reports:

- **Type 1 report**. A Type 1 report addresses the fairness of the vendor's description of the vendor's system and the suitability of the design of the vendor's controls to achieve the vendor's objectives.
- **Type 2 report**. A Type 2 report, which would be more useful, not only includes the Type 1 report information, but also reports on the operating effectiveness of the vendor's controls. So, it addresses not only whether the vendor has fairly described its system and the suitability of the design of the system to achieve its goals, but also whether it works in operation.

SOC 2 reports are said to be generally restricted. This presumably means their dissemination is restricted to management of the service organization, user entities that are customers of the service organization (such as plans, fiduciaries, and plan sponsors), and auditors of the users. In contrast, SOC 3 reports are general use reports that can be freely distributed.

SOC 3 report. A SOC 3 report is designed to meet the needs of users who do not have the need for or the knowledge necessary to make effective use of a SOC 2 report but need assurance about the controls at a service organization relevant to:

- Security
- Availability
- Processing integrity
- Confidentiality –or–
- Privacy

As between SOC 2 and SOC 3, the AICPA has indicated that if customers need to understand the details of the processing and controls at a service organization vendor, and the tests performed by the service auditor and the results, a SOC 2 report is the right choice. If customers do not have the need for, or the ability to understand, these details, a SOC 3 report may be an appropriate choice.

The AICPA has also developed a cybersecurity risk management reporting framework enabling organizations to communicate about the effectiveness of their cybersecurity risk management programs. This includes a new SOC for cybersecurity engagement, through which a CPA can report on an organization's "enterprise-wide cybersecurity risk management program." The resulting SOC for cybersecurity is intended, in part, to help business partners of the audited vendor gain a better understanding of the vendor's cybersecurity efforts. A starting place may be to ask prospective vendors in RFPs about the availability of SOC 2, SOC 3, or SOC for cybersecurity reports. As an alternative to a SOC report, plans might consider requesting a certification under the Health Information Trust Alliance (HITRUST).

Cybersecurity Assessment Tools

For recordkeepers and other vendors affiliated with financial institutions, ask for the results of their vulnerability assessment to cybersecurity risks under the Cybersecurity Assessment Tool developed by the Federal Financial Institutions Examination Council (FFIEC). This is a tool designed to help financial institutions identify risks and determine their cybersecurity preparedness. For more information, see ERISA Advisory Council, Cybersecurity Considerations for Benefit Plans at 3 (2016).

SEC Regulation S-P and FTC Red Flag Rules

With vendors that are investment advisors (or brokers, dealers, transfer agents, or investment companies), SEC Regulation S-P requires adopting policies and procedures reasonably designed to meet various security and confidentiality objectives. Certain financial institutions are required by the Federal Trade Commission (FTC) "Red Flag" rules to have and implement a written identity theft program. FTC: Fighting Identity Theft with the Red Flags Rule: A How-to Guide for Business (May 2013). For financial institutions and others subject to the SEC regulation or FTC Red Flag rules, ask about their compliance with those requirements.

For an example of an SEC enforcement action relating to cybersecurity and failing to meet the requirements of Regulation S-P, see the SEC, Administrative Proceeding Order, Morgan Stanley Cease and Desist (June 8, 2016). In that order, Morgan Stanley Smith Barney LLC agreed to pay a $1 million penalty to settle charges relating to the failure to protect customer information, some of which was hacked and offered for sale online. The SEC order found that Morgan Stanley failed to adopt written policies and procedures reasonably designed to protect customer data, and between 2011 and 2014 a then-employee impermissibly accessed and transferred to his personal server data relating to approximately 730,000 accounts. This data was ultimately hacked by third parties. For a summary of SEC cybersecurity enforcement actions, see SEC: Cybersecurity Enforcement Actions.

Vendor Contracts

When contracting with new vendors, consider incorporating into the contract elements of a typical HIPAA business associate agreement. These might include:

- Rules on who the vendor can communicate with (e.g., who the vendor can communicate with at the employer or other plan sponsor)
- How the vendor handles internal data at rest and data in motion (perhaps applying Department of Health and Human Services–approved technology standards for data in motion, including encryption)

- Breach notification obligations (including requiring the vendor to handle notifications to participants and other affected individuals)
- An obligation to impose similarly protective constraints on its subcontractors and vendors to whom it may disclose personally identifiable information
- The destruction, return, or other disposition of PII upon termination of the arrangement
- What uses of PII are permitted –and–
- Indemnification of the plan, fiduciaries, and employer or other plan sponsor if a breach occurs a violation of the law

In new vendor contracts, fiduciaries may also wish to require vendor representations, and indemnification protections, addressing all state and federal legal requirements, as well as industry standards, relating to security and privacy (and presumably other laws as well). Comprehensive representations and indemnification would presumably cover not only violations of the state privacy statutes mentioned above, but also federal laws governing particular industries, such as the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act, and the Fair and Accurate Credit Transaction Act.

On compliance with industry standards, it may be worth requesting a commitment to comply with International Organization for Standardization (ISO) Information Security Standards 27001 and 27002, and asking the vendor to maintain certification it has met these standards. See Int'l Organization for Standardization.

Request Reports from Existing Vendors

Though it may be more difficult, fiduciaries may wish to take steps with existing vendors like those described above for new vendors. So, for example, it may make sense to ask existing vendors for SOC reports, and incorporate into agreements the contractual provisions described above upon the renewal, extension, or amendment of existing agreements.

SAFETY Act

Plan sponsors may wish to consider retaining vendors that use technology having received designation or certification under the Support Anti-Terrorism by Fostering Effective Technologies Act of 2002, Pub. L. No. 107-296 (SAFETY Act). See Dep't of Homeland Security, Safety Act. Compliance with SAFETY Act standards may, however, not be cost-effective. See ERISA Advisory Council Report at 11.

Suggested Plan Sponsor Actions

Besides the steps required of third-party vendors, plan fiduciaries may wish to take internal steps to safeguard PII, including those affecting operations of the plan sponsor. These could include:

- Applying HIPAA-like policies to non-HIPAA data
- Becoming familiar with state statutes –and–
- Exploring cybersecurity insurance

Apply HIPAA Policies to PII

A reasonable and achievable model for improving internal security and privacy controls may be the plan sponsor's existing HIPAA privacy and security procedures. Not all of the standards in those procedures must be applied regarding retirement or other non-health plan data, but the plan sponsor might consider whether application of a

stripped-down version of those processes to PII might be appropriate. Something more robust might make sense regarding information that involves an individual's health or other information an employer could be accused of misusing (e.g., to fire an employee). The obvious example would be information relating to disability benefit claims. Showing that a manager who fired an employee had no access to information about the employee's disability could prove helpful should the employee make an Americans with Disabilities Act or ERISA Section 510 claim.

It may also make sense to borrow other, low-tech practices, from the employer's or other plan sponsor's HIPAA policies and procedures. These could include simple steps such as the routine use of locked file cabinets, shredding of documents, and not leaving papers with PII sitting at vacant desks or left at photocopying stations.

Review Compliance with State Statutes

The suggestions above relate primarily to satisfying fiduciaries' prudence obligation under ERISA. Because of the real possibility that generally applicable state statutes relating to privacy and security will not be preempted by ERISA, fiduciaries should become familiar with state laws that may apply to their plans. A good starting point would be to examine the statutes in force in the states in which the plan is situated or has participants.

Obtain Cybersecurity Insurance

Fiduciaries may wish to explore the possibility of purchasing insurance policies explicitly covering cybersecurity and privacy risks. In doing so, fiduciaries should carefully examine existing coverage they have under fiduciary liability insurance policies. The likelihood is that existing fiduciary liability insurance coverage will not cover risks relating to liability that results from state law causes of action (that are not preempted), as opposed to liability resulting from a breach of an ERISA fiduciary duty relating to a privacy or security breach. Importantly, cybersecurity insurance may provide coverage not only for liability resulting from a security breach, but may also help cover the costs of any required notifications and other recovery steps associated with a privacy or security breach, even if the breach has not, and may never, trigger a liability claim by an injured party.

For a further discussion about the benefits of cybersecurity insurance, see Why the Insurance Industry Cannot Protect Against Health Care Data Breaches, 19 J. Health Care L. & Policy 271, Part III.

Other Steps

For further suggestions about possible approaches for increasing privacy and security protections, particularly at the employer or other plan sponsor level (as opposed to at the vendor level), fiduciaries may wish to refer to the ERISA Council Report. See ERISA Advisory Council Report. The report includes a great deal of helpful information, including an appendix offering a framework and suggestions. These suggestions were influenced by the Cybersecurity Framework developed by the National Institute of Standards and Technology (NIST) of the U.S. Department of Commerce. Fiduciaries and plan sponsors may also wish to consult a NIST publication, Celia Paulsen & Patricia Toth, Small Business Information Security: The Fundamentals (2016).

RELATED CONTENT

Practice Notes

- Privacy Policies: Drafting a Policy
- ERISA Preemption
- Fundamentals of ERISA Fiduciary Duties

- HIPAA Privacy, Security, Breach Notification, and Other Administrative Simplification Rules
- Privacy and Data Security Considerations When Negotiating or Reviewing a Transaction or Agreement
- Request for Proposal Checklist (Retirement Plan Service Provider)

Checklists

- Data Breach Notification Enforcement and Penalties State Laws Chart

John Utz
Partner, Utz & Lattan

John Utz focuses exclusively on employee benefits and executive compensation law, including matters affecting pension, profit sharing, and 401(k) plans, ESOPs, Section 403(b) tax-sheltered annuities, Section 457 plans, stock options, nonqualified deferred compensation, incentive pay, severance pay, and health and welfare programs.

Mr. Utz is a Fellow in the American College of Employee Benefits Counsel and the American College of Tax Counsel. He is listed in The Best Lawyers in America and Superlawyers. Mr. Utz is active in the American Bar Association, having served as Chair of the Employee Benefits Committee of the Section of Taxation and having chaired multiple ABA subcommittees.