PRIVACY RISKS BEYOND HIPAA: RETIREMENT AND OTHER NON-HEALTH BENEFIT PLANS

2018 JOINT TE/GE COUNCIL EMPLOYEE PLANS & EXEMPT ORGANIZATIONS ANNUAL MEETING

FEBRUARY 22-23, 2018

University of Baltimore
Baltimore, Maryland

By:

John L. Utz, Esq.

UTZ & LATTAN, LLC
7285 W. 132nd St., Suite 320
Overland Park, Kansas 66213
(913) 685-7978 Direct Dial
(913) 685-1281 Telefacsimile
jutz@utzlattan.com

PRIVACY RISKS BEYOND HIPAA:
RETIREMENT AND OTHER NON-HEALTH BENEFIT PLANS

By
John L. Utz
Utz & Lattan, LLC
jutz@utzlattan.com
(913) 685-7978

TABLE OF CONTENTS

PRIVACY RISKS BEYOND HIPAA: RETIREMENT AND OTHER NON-HEALTH BENEFIT PLANS

By
John L. Utz
Utz & Lattan, LLC
jutz@utzlattan.com
(913) 685-7978

Introduction. The day will come when a retirement plan fiduciary is held liable for a security or privacy breach. It might be when participants' social security numbers end up in the wrong hands, and criminals use those numbers to impersonate participants in financial transactions or otherwise "steal" the participants' identities. Or perhaps through a lack of adequate security, a former spouse or other companion will wrongly take a distribution of a participant's retirement benefits.

This risk for retirement plan fiduciaries does not appear to be especially high today. But it is going to become meaningful, and probably sooner than we would hope. Soon enough, in fact, that fiduciaries of retirement and other non-health plans should begin now to bolster their processes for protecting participants' private information in the possession of plans, plan vendors, and the fiduciaries themselves.

One risk for fiduciaries is the possibility courts will conclude that ERISA's prudence requirement imposes an obligation to do something substantial to protect the privacy of participants. In particular, one can imagine a day when courts will require fiduciaries to take carefully considered steps to reduce the risk of private information that can be used to identify participants being accessed by unauthorized parties or otherwise being misused. Courts do not yet seem to hold fiduciaries to a high standard in this regard, but 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 importantly, the consciousness of judges – the standards for what is prudent to protect "personally identifiable information" (or "PII")'[1] may become stricter in *pari passu*. As courts and the Department of Labor have told us for some time, ERISA's prudence requirement is mostly about process – that is, following a good process. It is less about the result, and more about diligence in considering and addressing concerns. As the processes for reducing risk security and privacy rules become better developed and more commonly utilized by businesses, governments, and individuals, it seems inevitable that what is considered prudent in handling PII will change accordingly.

[1] One definition of personally identifiable information comes from the Office of Management and Budget. OMB defines PII as:

> [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 a 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."

In a bit of perversity, news that the increasing frequency and severity of security breaches may herald a heightened obligation to protect the PII of benefit plan participants carries with it an understanding that it will be virtually impossible to provide assurance that no breach of security will occur, or that PII will not be misused. After all, the National Security Agency (the "NSA") – which describes itself as "the world leader in cryptology," is the manager for U.S. government systems that "contain classified information or are otherwise critical to U.S. military or intelligence missions," and the work of which gives the NSA what it calls "end-to-end insights into . . . cyber best practices" – has been hacked.[2] According to press reports, the NSA, "America's . . . most secretive intelligence agency," has been "deeply infiltrated."[3] In a *New York Times* article describing the NSA breach the *Times* said "the [a]gency regarded as the world's leader in breaking into adversaries' computer networks failed to protect its own." And the same article reported that some intelligence officials believe America's cyber defense has been left "dangerously porous."[4]

Not only does the fact of the NSA breach suggest that benefit plan fiduciaries cannot assure data security, what has been stolen from the NSA may itself increase the threat to benefit plans (and the rest of the earth). That is because the stolen materials include sophisticated tools with software "to bypass computer firewalls, penetrate Windows, and break into the Linux systems most commonly used on Android phones."[5] These tools are apparently for sale through subscriptions to a "monthly dump service" of stolen NSA software and data.[6]

In addition to the demoralizing hack of the NSA, there has reportedly been a "hemorrhage of hacking tools and secret documents from the Central Intelligence Agency's Center for Cyber Intelligence."[7] Adding to the sense that one cannot prevent security breaches, the Securities Exchange Commission's computer system was hacked in 2016.[8] And not to pile on, but according to press reports a 2013 Yahoo breach affected the information of all 3 billion of its customers;[9] Deloitte,[10] one of the big four accounting firms, has been hacked; and a 2014 J.P. Morgan Chase & Co. hack compromised the accounts of 76 million households and seven million small businesses.[11] According to one source, 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.[12] As to the Yahoo breach, the hackers reportedly obtained names, birthdates, phone numbers, and passwords of users that were "encrypted with security that was easy to crack." They also obtained security questions and backup email addresses used to reset lost passwords. The *New York Times* characterized this as "valuable information for someone trying to break into other

---

[2] As to the description of the NSA's role, see the agency's website at www.nsa.gov. As to the breach of NSA security, see "Deep Security Breach Cripples N.S.A.," *New York Times*, Nov. 13, 2017, p. A1.
[3] "Deep Security Breach Cripples N.S.A.," *New York Times*, Nov. 13, 2017, p. A1.
[4] *Ibid*.
[5] *Ibid*.
[6] *Ibid*.
[7] *Ibid*.
[8] "SEC Gets Scrutiny for Slow Response to Hack," *Wall Street Journal*, Sept. 22, 2017, p. A1.
[9] "All 3 Billion Yahoo Accounts Were Affected by 2013 Attack," New York Times.com (Oct. 3, 2017), available at https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html.
[10] https://www.theguardian.com/business/2017/sep/25/deloitte-hit-by-cyber-attack-revealing-clients-secret-emails,
[11] "JPMorgan Chase Hacking Affects 75 Million Households," *New York Times*, Oct. 2,2 014.
[12] https://www.theguardian.com/business/2017/oct/10/deloitte-hack-hit-server-containing-emails-from-across-us-government.

accounts owned by the same user, and particularly useful to a hacker seeking to break into government computers around the world."[13]

Given the NSA and CIA breaches alone – including the resulting sale of sophisticated hacking tools from the NSA toolbox – one might wonder not only whether there is any point in trying to improve plan data security, but also whether participants or others seeking to hold fiduciaries liable for breaches can successfully argue they were harmed by a breach. Couldn't a plan fiduciary convincingly argue that for participants complaining they have been harmed by, say, the release of their social security numbers, any harm they have suffered is just as likely to have been the result of some other breach of their information, and they can't possibly establish that they were harmed (or will be harmed) by the plan's breach? Notably in this regard, the hack of Equifax Inc. alone reportedly may have exposed sensitive information about more than 140 million Americans, including core personal information, such as names, addresses, dates of birth, and social security numbers. [14] In addition, credit card numbers for approximately 209,000 consumers and certain "dispute" documents with personal identifying information for approximately 182,000 consumers were improperly accessed.[15]

This 140 million number relating to the Equifax hack is about 40 percent of the total population of the United States, and more than half of the U.S. population age 16 and over. Given that social security numbers are frequently used by those engaged in identity theft, 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, a participant can't establish he or she suffered an injury as required to bring a lawsuit. The argument would be that to bring suit 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 in order to have recourse under ERISA.[16] And even if state claims are allowed to proceed in state court – for example where there is no complete preemption and state law claims are not preempted by ERISA – perhaps there are no losses or damages on which a participant can collect.

***Anthem* and Pleading Damages**. As it turns out, at least one court has already rejected this very defense – that the ubiquity of security beaches precludes plan participants from establishing they have been harmed by a plan-related breach. The case involved a 2015 cyber attack on Anthem's databases. That attack resulted in the theft of information concerning 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.[17] Although the case involves a health plan, and this article is focused on risks relating to retirement and other plans not subject to the standards of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the legal analysis as to whether a

[13] "All 3 Billion Yahoo Accounts Were Affected by 2013 Attack," New York Times.com (Oct. 3, 2017), available at https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html.
[14] "'We've Been Breached,' Inside the Equifax Hack," *Wall Street Journal*, Sept. 18, 2017, p. A1.
[15] www.equifaxsecurity2017.com/consumer-notice.
[16] *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).
[17] Notice of Anthem Data Breach Class Action Settlement, U.S. District Court for the Northern District of California, available at www.databreach-settlement.com.

participant is damaged by a privacy breach should generally be same with respect to all types of benefit plans.

A settlement of the Anthem case was announced in June of 2017. Under that settlement, Anthem agreed to pay $115 million. In doing so, Anthem settled various class action lawsuits that had been consolidated in the federal District Court for the Northern District of California through the Judicial Panel on Multidistrict Litigation. The consolidated cases generally alleged that the defendants failed to adequately protect Anthem's data systems, failed to disclose to customers that Anthem did not have adequate security practices, and failed to timely notify customers of the data breach.

Before Anthem settled the cases, a district court addressed whether participants had adequately pleaded that they had been damaged. The court addressed this damage pleading issue as part of a lengthy decision concerning the defendants' motion to dismiss many state law claims, including privacy claims, as well as breach of contract, unfair competition, and unjust enrichment claims. Specifically, in *In re Anthem, Inc. Data Breach Litigation*,[18] the court considered defendants' argument that the plaintiffs had not sufficiently pleaded damages for loss of value of what the court termed "personal identification information" or "PII." The court concluded that the plaintiffs had sufficiently pleaded damages. In doing so, the court cited a Ninth Circuit decision, as well as several district court decisions, though those cases did not involve employee benefit plans. In one of those cases, the Northern District of California (the same court issuing the decision in *Anthem*) itself concluded that plaintiffs had sufficiently pleaded economic injury by claiming "that the[ir] PII was stolen and posted on file-sharing websites for identity thieves to download."[19]

The defendant in *Anthem* argued that the earlier decisions cited by the court (the non-benefit plan cases) effectively imposed two pleading requirements on the plaintiffs – specifically, that they must plead "both that there was a 'robust' market for [Plaintiffs' PII] *and* that [P]laintiffs had been financially harmed by [the data breach by] usurping their ability to sell that information themselves." The court rejected the argument that there is a requirement 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 that 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 were to apply, 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." The complaint continued, "[w]ith access to an individual's [PII], criminals can do more than just empty a victim's bank account – they can also commit various types of fraud . . . [they] may obtain a job using the victim's Social Security Number." The court found that these allegations could be read to infer that an economic market existed for the plaintiffs' PII, and that the value of the plaintiffs' PII decreased as a result of the Anthem data breach. The court found support for this conclusion in a Seventh Circuit decision concerning a breach of a retailer's database, where the Seventh Circuit said "[p]resumably, the purpose of [a] hack is, sooner or later, to make fraudulent charges or

[18] 2016 U.S. Dist. LEXIS 70594 (N.D. Cal. 2016).
[19] *Corona v. Sony Pictures Entertainment, Inc.*, 2015 U.S. Dist. LEXIS 85865 (N.D. Cal. 2015).

assume those consumers' identity."[20] The Seventh Circuit underscored the point with the rhetorical question "[w]hy else would hackers break into a store's database and steal consumers' private information?"

No Article III Standing. Not all courts have been as quick to conclude that those making privacy claims based on the theft of private information can establish Article III standing. As an example, consider *Cox v. Valley Hope Ass'n.*[21] There, a district 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.

A putative class action was filed against the treatment center in state court, asserting various claims, including those based on breach of contract, negligence, breach of fiduciary duty, and violation of a state consumer anti-fraud statute. The case was removed to federal district court, and the district court dismissed the suit on Article III grounds. The plaintiff argued, among other things, that he had "suffered damages, including and without limitation, loss of privacy, confidentiality, embarrassment, humiliation, loss of income, [and] loss of enjoyment of life." But the plaintiff offered little more by way of explanation, including no facts suggesting that his privacy was actually invaded, he actually suffered embarrassment or humiliation, or he spent any monies as a result of the laptop theft. The alleged injuries were, therefore, conclusory (and as a consequence, inadequate).

The court treated more seriously the named plaintiff's argument that he had been harmed because there is a "real and serious threat that his personal data will be misused" – that is, that he was at a heightened risk for future identity theft. To have Article III standing, though, the threat must be "imminent," which means it must not be "too speculative" and must be "certainly impending." The court found the claims as to the risk of future identity theft too speculative to afford Article III standing.

The court then addressed a further argument that the plaintiff was injured – specifically, that he overpaid for privacy protections promised by the treatment facility. But the court concluded that parties making this argument must allege they "overpaid for something – either the core product or an ancillary security service – for which they had expressly bargained." That was not the case here because the plaintiff did not allege the addiction treatment services he received from the treatment center had been diminished as a result of the laptop theft. Nor did he claim that he specifically paid for security protection.

Because the named plaintiff in the putative class action lacked Article III standing, the suit could not be brought in federal court. The case was therefore remanded to Missouri state court where it was originally filed.

State Law. 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.

[20] *Remijas v. Neiman Marcus Gr., LLC*, 794 F.3d 688, 693 (7th Cir. 2015).
[21] 2016 U.S. Dist. LEXIS 119663 (W.D. Mo. 2016).

Almost all states have privacy laws. But most are not comprehensive in scope. Most states impose notification requirements in the event of a security breach. Forty-eight states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have some form of such a notification requirement.[22] Most of these breach notification laws are, however, to be enforced by the state attorney general, and do not provide for a private right of action.

At least 32 states and Puerto Rico have laws requiring that personal identifying information be destroyed, disposed of, or otherwise made unreadable or undecipherable, once it is no longer to be retained.[23] Of greater concern than the breach notification and data disposal statutes, at least 13 states impose requirements concerning the maintenance of reasonable security procedures and practices in connection with personal information relating to the states' residents.[24] And a number of states have legislation restricting the use of social security numbers, which are still utilized in the administration of some retirement plans.[25]

The California Example. As noted above, some states not only impose breach notification requirements and obligations concerning the disposal of PII, but also impose standards concerning the maintenance of security procedures and practices. One example is a California statute that requires companies that "own, license, or maintain" personal information (about Californians) to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."[26] Personal information for this purpose includes an individual's first name or first initial and his or her last name, in combination with his or her (a) social security number, (b) account number, in combination with any required security code, access code, or password that would permit access to an individual's financial account, (c) medical information, or (d) health insurance information, when either the name or the data elements are not encrypted or redacted.[27] Personal information also includes a user name or email address in combination with a password or security question and answer that would permit access to an online account.[28]

As noted, the California statute applies to companies that "own, license or maintain" personal information. The terms "owned" and "licensed" are intended to reach a business that retains personal information as part of its "internal customer account" or for the purpose of using

---

[22] For a listing of these jurisdictions and citations to the relevant statutory provisions, see, http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

[23] For a listing of the jurisdictions with data disposal laws, and citations to the relevant statutes, see, http://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx.

[24] For a listing of states with such data security laws, and citations to the relevant statutory provisions, see, http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx.

[25] See "Social Security Numbers: Federal and State Laws Restrict Use of SSNs, Yet Gaps Remain," US Government Accountability Office, GAO-05-1016T, Appendix III for examples of state legislation restricting the use of social security numbers, as well as these two links: http://consumersunion.org/news/state-laws-restricting-private-use-of-social-security-numbers/ and http://www.ncsl.org/research/financial-services-and-commerce/social-security-number-2010-legislation.aspx.

[26] Cal. Civ. Code ¶ 1798.81.5(b).

[27] Cal. Civ. Code ¶ 1798.81.5(d)(1)(A).

[28] Cal. Civ. Code ¶ 1798.81.5(d)(1)(B).

that information in transactions with the person to whom the information relates.[29] The term "maintained" is intended to reach a business that "maintains," personal information, even though it does not own or license that personal information.[30]

Other State Law Claims, Including Under Common Law. 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. Often, our reflexive reaction to state law claims is that they are surely preempted by ERISA. But the modest caselaw authority to date suggests this visceral "analysis" may be overly optimistic. The preemption argument may be strongest where the security breach or misuse of private information occurs in connection with a function that is central to the administration of a benefit plan. Where, though, the complaint concerns activity that is not core to the administration of a benefit plan, the ERISA preemption argument is weaker. An example of this is seen in *Darcangelo v. Verizon Communications., Inc.*[31] In *Darcangelo,* 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. The participant complained that the third party administrator solicited private medical information from medical providers about her mental health and medical treatment for the sole purpose of helping her employer establish that she posed a sufficient threat to her co-workers to warrant her discharge.

The Fourth Circuit refused to dismiss on ERISA preemption grounds state law claims for invasion of privacy, negligence, violation of a state unfair and deceptive trade practices statute, and violation of a state medical record confidentiality statute. In doing so, the court concluded that the key question was whether the administrator obtained the plaintiff's medical information either in the course of processing the plaintiff's benefits claim or in the course of performing any of its administrative duties under the plan. If so, the Fourth Circuit said, these claims would be preempted. 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 posed a threat to her co-workers, the four state law claims would not be related to the plan, and therefore would not be preempted. In ruling on the defendants' motion to dismiss, the Fourth Circuit was required to read the complaint in the light most favorable to the plaintiff, and under that constraint the court concluded that the plaintiff had alleged that the administrator's conduct was not related to its duties under the plan. The court therefore refused to dismiss the privacy, negligence, unfair trade practices, and medical record confidentiality claims on ERISA preemption grounds.

The plaintiff also brought a breach of contract claim. But because the contract in question was a plan subject to ERISA, that claim was "clearly" preempted. It was clearly preempted because the breach of contract claim was "an alternative enforcement mechanism" to ERISA Section 502. Specifically, since ERISA permits participants to bring an action to enforce their

[29] Cal. Civ. Code ¶ 1798.81.5(a)(2).
[30] *Ibid.*
[31] 292 F.3d 181 (4th Cir. 2002).

rights under the terms of a plan, an action to enforce the terms of a contract, where that contract is a plan subject to ERISA, is of necessity an alternative enforcement mechanism for ERISA Section 502. As such, the breach of contract claim was "related to" an ERISA plan and preempted by Section 514. Further, as an alternative enforcement mechanism the claim was not only preempted but also completely preempted so as to justify removal of the action from state to federal court.

In explaining its preemption analysis, the court cited the Supreme Court chestnut *Mackey v. Lanier Collection Agency & Svcs., Inc.*,[32] and in particular that case's language suggesting that ERISA was not meant to excuse tortious conduct. In *Mackey*, the Supreme Court said many "lawsuits against ERISA plans for run-of-the-mill state-law . . . torts committed by [the] ERISA plan" are not preempted, even though they "obviously affect [ ] and involve ERISA plans and their trustees." The Fourth Circuit melded this sentiment from *Mackey* with the Supreme Court's decision in *Pegram v. Herdrich*,[33] saying:

> [O]ur "doubt that Congress intended the category of fiduciary administrative functions to encompass" tortious conduct by a plan administrator that is completely unrelated to its duties under the plan "hardens into conviction when we consider the consequences that would follow from [the defendants'] contrary view." Under the defendants' view, ERISA administrators would enjoy blanket immunity -- at least from damages under state tort law -- for any manner of wrongful conduct aimed at plan participants and beneficiaries, regardless of how unrelated that conduct is to the ERISA plan. We cannot imagine that Congress would have wanted such a result. As our court has explained, state common law torts such as invasion of privacy and negligence are traditional areas of state authority, and "federalism concerns strongly counsel against imputing to Congress an intent" to preempt large swaths of state law "absent some clearly expressed direction." (Citations to *Pegram* and the Fourth Circuit's decision in *Custer v. Sweeney* omitted.)

The Fourth Circuit offered this further instruction about the centrality of the plan administration nexus:

> ERISA, as its goals indicate, does not seek to preempt all state laws that might apply to an ERISA plan administrator, but only those laws that undermine the "nationally uniform *administration* of employee benefit plans." (emphasis added). When an ERISA plan administrator takes action entirely unrelated to the administration of the plan, liability for that action does not threaten the uniformity of plan administration. Likewise, while ERISA establishes "'standards of conduct, responsibility, and obligation for fiduciaries,'" it does not preempt general state laws covering nonfiduciary acts unrelated to an ERISA plan. (Citations omitted.)

Dishman. *Darcangelo* is one of the two leading cases concerning ERISA's preemption of state privacy laws. The Fourth Circuit in *Darcangelo* cited the other leading case, an earlier Ninth Circuit decision also involving a disability plan. That was *Dishman v. UNUM Life Ins. Co. of Am.*[34] *Dishman* concerned a claim less far removed from proper plan administration than the claim

[32] 486 U.S. 825 (1988).
[33] 530 U.S. 211 (2000).
[34] 269 F.3d 974 (9th Cir. 2001).

in *Darcangelo*, and therefore perhaps offering a stronger argument for preemption. But, alas, it was not a strong enough argument, and the Ninth Circuit in *Dishman* refused to dismiss the plaintiff's state law invasion of privacy claim on ERISA preemption grounds. Recall that in *Darcangelo* the allegation was that a plan administrator was doing the employer's bidding, not for benefit plan purposes but instead for a purpose relating to the plan participant's employment. In *Dishman* that was not the case. There, the claim was that the long term disability insurer acted improperly in investigating whether the plaintiff was disabled for benefit eligibility purposes. The Fourth Circuit in *Darcangelo* ably summarized *Dishman* this way:

> A Ninth Circuit case, *Dishman v. UNUM Life Ins. Co. of Am.*, provides an example of a non-preempted state tort claim that was asserted by an ERISA beneficiary against the plan administrator. In that case the beneficiary brought an action for invasion of privacy against the plan administrator, alleging that the administrator's claims investigator had wangled out personal information about the beneficiary by, among other things, impersonating the beneficiary to third parties, falsely claiming to be a bank loan officer, and misrepresenting to the beneficiary's neighbors that he had volunteered to coach a basketball team. The court rejected the idea that "a plan administrator could 'investigate' a claim in all manner of tortious ways with impunity." Because the beneficiary simply alleged "garden variety torts which only peripherally impact daily plan administration," the court held that the state invasion of privacy law was not preempted. (Citations omitted.)

It is pretty clear courts are not keen on excusing tortious behavior on ERISA preemption grounds. Nor laws of general applicability. As to the latter, the Ninth Circuit in *Dishman* cited the Supreme Court's decision in *New York Conference of Blue Cross & Blue Shield Plans v. Travelers Ins. Co.*,[35] where the Supreme Court said "pre-emption 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."

The fact that the complained of conduct in *Dishman* allegedly occurred in the course of 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."

***Anthem* Redux**. Earlier, I mentioned the *Anthem* litigation[36] for the proposition that plaintiffs may be able to argue they have been financially harmed by the mere theft of their personally identifiable information. Although *Anthem* involved health insurance, and this article is about plans not subject to HIPAA, *Anthem* is nevertheless instructive as well on the preemption issue. As earlier noted, Anthem suffered a massive data breach. In response to a rash of claims, Anthem and other defendants argued that certain of those claims were preempted. Among them were state breach of contract and unjust enrichment claims. The breach of contract claims were based in part on assertions that Anthem and other defendants promised their members that members' PII would be protected. The defendants offered those promises through privacy notices,

[35] 514 U.S. 645 (1995).
[36] *In re Anthem, Inc. Data Breach Litigation*, 2016 U.S. Dist. Lexis 70594 (N.D. Cal. 2016).

online website representations, and other advertising. As an example, Anthem's privacy policy allegedly stated the following:

> Anthem Blue Cross and Blue Shield maintains policies that protect the confidentiality of personal information, including Social Security numbers, obtained from its members and associates in the course of its regular business functions. Anthem Blue Cross and Blue Shield is committed to protecting information about its customers and associates, especially the confidential nature of their personal information.
>
> * * *
>
> Anthem Blue Cross and Blue Shield has in place a minimum necessary policy which states that associates may only access, use or disclose Social Security numbers or personal information to complete a specific task and as allowed by law.
>
> Anthem Blue Cross and Blue Shield safeguards Social Security numbers and other personal information by having physical, technical, and administrative safeguards in place.

The court held that California contract law claims were not preempted. In its preemption analysis for the breach of contract claim, the district court looked to the Supreme Court's decision in *Gobielle v. Liberty Mut. Ins. Co.*,[37] where the Supreme Court noted that:

> [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. (Internal quotation marks and ellipses omitted.)

In the quoted language above, the Supreme Court describes 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.[38]" 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 court said the analysis was tougher, but the state breach of contract, unjust enrichment, and deceptive business practices

[37] 136 S. Ct. 936 (2016).
[38] *Gobeille v. Liberty Mut. Ins. Co.*, 136 S. Ct. 936 (2016).

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 that have a connection with ERISA plans by "mandat[ing] employee benefit structures or their administration" (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. Offering detail on the types of laws that have a connection with ERISA plans, the court quoted from the Second Circuit's decision in *Gerosa v. Savasta & Co.*,[39] 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."

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." 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 <u>benefits</u>. As the court put it, there is no suggestion in ERISA that "protecting customer PII should be considered an ERISA benefit." 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.*,[40] 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. In *Anthem* the plaintiffs did not make a claim for the payment of medical or healthcare expenses. They instead alleged that the defendants failed to comply with certain privacy obligations, "a legal area where ERISA is silent."

In an observation that may have shown its hand, 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." The defendants were, therefore, asking the court to "break new ground" to find that the general "presumption against preemption" is overcome in a field where it has never before been applied. The court declined to do that, refusing to dismiss the state law claims as preempted.

<u>Back in the Day</u>. Interestingly, although I have asserted that *Darcangelo* and *Dishman* are the leading cases, the ERISA preemption analysis of privacy claims dates back to at least 1993. That is when the Sixth Circuit decided *In re General Motors Corp.*[41] There, the court held that invasion of privacy, breach of contract, and misrepresentation claims relating to a failure to keep employee assistance plan information confidential <u>were</u> preempted by ERISA (and also by the Labor Management Relations Act). This, of course, is in contrast to the results in *Darcangelo* and *Dishman* where the state law claims were not preempted. The Sixth Circuit's analysis was sparse, but the court said the claims were preempted even though the plaintiff did not seek to be made whole by receiving an award of benefits the EAP was designed to provide.[42] In other words, the

[39] 329 F.3d 317 (2d Cir. 2003).
[40] 761 F.3d 232 (2d Cir. 2014).
[41] 3 F.3d 980 (6th Cir. 1993).
[42] The Third Circuit has also held that the Labor Management Relations Act (the "LMRA") preempted state common law tort claims, including invasion of privacy, in a non-employee benefits case called *Kline v. Sec. Guards, Inc.*, 386 F.3d 246 (3d Cir. 2004).

plaintiff was asking for something different (or more) than benefits, yet the claims were still preempted.

Disguising a Benefit Claim. If the court in *Anthem* is right, the preemption question becomes one of whether the laws at issue implicate the administration of benefit plans. Clever pleading should not, however, save a claim that should, in fact, preempted. We see justice done in this regard in *Hogan v. Jacobson,*[43] 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 statelaw 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.

Later in the same year, the Sixth Circuit reached a similar conclusion in *Milby v. MMC, LLC,*[44] where the court held that a negligence per se claim against a medical record reviewer in a disability benefit dispute was preempted by ERISA.

More Preemption of State Law Claims: *Premera*. For another district court decision holding that state common law and statutory claims relating to a security breach of personally identifiable information were not preempted, see *In re Premera Blue Cross Customer Data Sec. Breach Litig.*[45] *Premera* involved a putative class action against a Blue Cross organization after its public disclosure that its computer network had been breached. The plaintiffs alleged the breach compromised confidential information of approximately 11 million current and former health plan members, "affiliated members," and employees of Premera itself. The plaintiffs alleged that the compromised confidential information included names, dates of birth, social security numbers, member identification numbers, mailing addresses, telephone numbers, email addresses, medical claims information, financial information, and other protected health information.

As in *Anthem*, the state contract claims were based in part on standard plan documents. These included policy booklets the plaintiffs alleged contained affirmative misrepresentations about the defendant's protection of participants' privacy, such as promises that Premera would make sure participants' personal information stayed confidential. Other documents allegedly misrepresenting the protection in place for sensitive information were Premera's confidentiality policy and its privacy notice provided to members.

The court held that the plaintiffs had adequately alleged an express contract by reason of the policy booklet and privacy notice, and found that representations in the privacy notice were sufficiently specific for misrepresentation claims and a breach of contract claim to move forward. The court even concluded that plaintiffs had sufficiently alleged a claim for a breach of an implied-in-fact contract, where they asserted that by "providing their Sensitive Information, and upon

[43] 823 F.3d 872 (6th Cir. 2016).
[44] 844 F.3d 605 (6th Cir. 2016).
[45] 2017 U.S. Dist. Lexis 18322 (D. Ore. 2017).

Defendant's acceptance of such information, [the parties] entered into implied-in-fact contracts for the provision of data security, separate and apart from any express contracts."

The *Premera* court held that the state statutory and common law claims were not preempted by ERISA. Although this was the same result as in *Anthem*, the court diverged from the *Anthem* court's analysis. Before explaining how the court diverged from the *Anthem* analysis, I would like us to pause for a moment to meditate on the difference between "complete preemption" and "preemption." I want to do so because 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, seemingly conflating the two concepts (which is unfortunate). As the reader likely knows, complete preemption is a jurisdictional concept, relating to whether claims made in state court – and ostensibly concerning 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."[46] Stronger, the "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 certainly be preempted without the defendant having a right under the complete preemption doctrine to remove a state court action to federal court. In other words, it is not necessary for a claim to be completely preempted in order 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. As noted 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.

One wonders if the reason some federal district courts, when attempting to address ERISA preemption, seem to lean on complete preemption cases is that they assume if claims are completely preempted they are, *a fortiori*, also preempted. This is sort of true. In other words, complete preemption probably implies preemption, or something similar – the "something similar" being that 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*,[47] 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 (1) the plaintiff could have brought the claim under ERISA Section

[46] *Aetna Health Inc. v. Davila*, 542 U.S. 200 (2004).
[47] See n. 46 above.

502(a)(1)(B), and (2) no other independent legal duty is implicated by the defendant's actions (citing *Metropolitan Life Ins. Co. v. Taylor*[48]):

> 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))

So, complete preemption means the claims are preempted somehow. But 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 the question 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.

With this digression exhausted, and begging your pardon for it, let me return to the court's analysis in *Premera*, and note how it differs from the approach taken by the court in *Anthem*. The *Premera* plaintiffs argued that data protection is not a "benefit" as that term is used in ERISA and therefore that they could not bring a claim under Section 502(a). If that is right, the first prong of the *Davila* test for complete preemption would not be met. And even if data protection is an ERISA benefit, the plaintiffs argued complete preemption would not apply because Premera's duty to protect the plaintiffs' "sensitive information" arises independently from the ERISA plan documents. If that is right, the second prong of *Davila's* test for complete preemption would also not be met. And if either prong is not met, there is no complete preemption under *Davila*.

As to the first of the plaintiffs' arguments – whether they could bring a claim under Section 502(a) – the court noted that in *Anthem* the Northern District of California found that data security was not a "benefit" as that term was used in ERISA. So far, so good, for the plaintiffs. And the *Anthem* court also concluded that all potential claims under Section 502(a)(1)(B) necessarily involve a "benefit." But the court in *Premera* said that is not true. It acknowledged that two of the three types of claims under Section 502(a)(1)(B) concern benefits – recovering benefits due under the plan, and clarifying rights to future benefits under the terms of the plan. But the third type of claim under that section involves enforcing rights under the terms of as plan. And the *Premera* court said this latter category allows a participant or beneficiary to enforce his or her rights under the plan, without reference to "benefits." The court concluded that at least some of the claims could have been brought under Section 502(a), thereby satisfying the first prong of the *Davila* test for complete preemption.

Even though the first prong of the *Davila* test for complete preemption was met, the second was not. One might assume the court would, as a consequence, hold merely that at least some of the state claims were not subject to <u>complete</u> preemption. But, oddly, the court jumped to the conclusion that the claims were not preempted. This is frustrating. It is not at all clear that complete preemption was even an issue before the court. Remember, complete preemption involves a jurisdictional question of whether removal to federal court is appropriate. Perhaps the

[48] 481 U.S. 58 (1987)

court thought if there were no complete preemption, the claims could not be preempted. But this would clearly be wrong. As noted earlier, if there is complete preemption, claims that serve as the basis for that complete preemption are necessarily preempted (or, perhaps, transformed into federal claims). But it is certainly not true that a lack of grounds for complete preemption means the claims are not preempted by ERISA. Put differently, state law claims may be preempted by ERISA without there being grounds for removing the action from state to federal court on a complete preemption basis.[49]

I am done, for the moment, venting about the *Premera* court's conflation of *Davila* complete preemption with the question at hand, conflict preemption. So, let's return to the court's conclusion that the state law claims were not preempted. The court reached this conclusion because the second *Davila* prong (for complete preemption) was not met. That second prong is the requirement that there be no independent duty implicated by the defendant's actions. Premera in fact did have a duty independent from the ERISA plan to reasonably and adequately protect the plaintiffs' data privacy. If the question were whether removal to federal court was warranted on complete preemption grounds, this would mean the second part of the *Davila* test had not been met. But the court focused on the independent duty prong for purposes of "simple" (that is, conflict) preemption. There was an independent duty asserted because the plaintiffs' allegations were not solely and entirely dependent on the ERISA plan. Instead, the plaintiffs alleged that Premera had a duty independent of the plan to protect their "sensitive information" under state law, HIPAA, and industry standards, no matter what was contained in the health insurance contracts.

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." The plaintiffs had sufficiently alleged an "independent legal duty separate from the ERISA plan" implicated by the defendant's alleged action, so 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 – the court summed up with language that may point to a fair rule of thumb, redolent of the Supreme Court's old *Mackey* decision. 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. (Again, the court actually said the claims were not "completely preempted," but it seemed also to mean "not preempted" since the case did not appear to involve a dispute over jurisdiction of a state court (and removal to federal court), and since the court in the second paragraph of the opinion refers to a motion to dismiss claims on preemption grounds.)

Rose v. HealthComp. Inc. As we noted earlier, although this article is about privacy risks relating to retirement and other plans not subject to HIPAA, the extant body of law concerning the preemption of privacy claims is populated with quite a few cases involving health plans. In another of those cases, and one with facts not too dissimilar to those in *Darcangelo* above, a district court

[49] *See, e.g., Metropolitan Life, Ins. Co. v. Taylor*, 481 U.S. 58, 64 (1987) ("ERISA pre-emption, without more, does not convert a state claim into an action arising under federal law"); *Franchise Tax Board of Cal. v. Construction Laborers Vacation Trust for Southern Cal*., 463 U.S. 1, 25-27 (1983); *Giles v. NYL Care Health Plans, Inc.*, 172 F.3d 333, 337 (5th Cir. 1999); *Dukes v. U.S. Healthcare, Inc.*, 57 F.3d 350, 355 (3d Cir. 1995).

considered invasion of privacy and unfair business practice claims relating to a health plan third party administrator's alleged disclosures to the plaintiff's employer. The case is *Rose v. HealthComp, Inc.*[50] The plaintiff in *Rose* complained that she was fired from her job after the TPA sent to her employer reports about her need for a liver transplant. The TPA allegedly assigned a nurse case manager to keep the plaintiff's healthcare claim costs down, and this nurse told the employee she would help the employee navigate the medical process. The nurse case manager allegedly had the employee sign a form authorizing the TPA to access the employee's medical records, but the employee was not told her medical information would be shared with her employer. The plaintiff claimed the TPA then sent reports about her medical condition to her employer on a monthly basis for approximately nine months, and these reports included information about her need for an expensive liver transplant.

The plaintiff sued the TPA, alleging invasion of privacy and unfair business practices in violation of California law. She filed her lawsuit in state court, but the defendant attempted to remove the case to federal district court. The district court ruled that the defendant had no right to remove the case because the claims were not completely preempted by ERISA. The court not only held that the claims were not completely preempted, it also concluded that they were not preempted. The facts were similar to those in *Darcangelo* (where claims were preempted) in that the plaintiff in *Darcangelo* complained that she had been terminated by reason of the disclosure of private health information. But *Rose* was different because the alleged disclosure occurred in connection with duties relating to a health plan subject to ERISA. The allegation in *Darcangelo* was instead that the disclosure was made solely for the purpose of showing that the plaintiff was a threat to her co-workers, and was not in connection with the provision of benefits.

As with a number of other cases, the *Rose* court was not very precise in distinguishing between the jurisdictional concept of complete preemption and the question whether claims would fail in any forum because they were preempted by ERISA. The context of the opinion was the jurisdictional question of whether removal had been appropriate. So, complete preemption was the primary focus of the court's analysis. And in this regard the court cited Ninth Circuit precedent[51] reciting the *Davila*[52] two part test for determining whether a state law cause of action is completely preempted by ERISA Section 502(a). The *Rose* court described the complete preemption standard by quoting the Ninth Circuit as follows: "A state-law cause of action is completely preempted if (1) 'an individual, at some point in time, could have brought the claim under ERISA § 502(a)(1)(B),' and (2) '[ ] there is no other independent legal duty that is implicated by a defendant's actions.'" Both prongs of this test must be satisfied for there to be complete preemption. Infuriatingly, the court in the very next sentence immediately confused the jurisdictional complete preemption issue with the question whether claims are preempted, saying "in determining whether Plaintiff's cause of action here are preempted by ERISA, the Court applies the two prong test set forth in [the Ninth Circuit complete preemption precedent] as set forth above." Oh, well.

The court held that the first prong of the *Davila* test for complete preemption – that the claim could have been brought under ERISA Section 502(a)(1)(B) – was met. That is because the

[50] 2015 U.S. Dist. Lexis 104706 (E.D. Cal. 2015).
[51] *Fossen v. Blue Cross & Blue Shield of Montana, Inc.*, 660 F.3d 1102 (9th Cir. 2011).
[52] See n. 46 above.

plaintiff alleged that in providing personal medical information to her employer the defendant did not act in the interest of employees and their beneficiaries, and this caused the court to conclude that the plaintiff's privacy and unfair business practice causes of action could be brought as a breach of fiduciary duty claim under ERISA Section 502. The first prong of the *Davila* test for complete preemption was therefore met. Oh, my, I know you must be weary of my nitpicking district court decisions, but it is hard to resist here. Remember, the first prong of the *Davila* test concerns whether the claim could have been brought under Section 502(a)(1)(B). The *Rose* court said this was the case because the plaintiff's complaint could have been brought as a breach of fiduciary duty claim. The problem is that fiduciary duty claims are generally brought under Section 502(a)(2), not Section 502(a)(1)(B) as required under the first prong of the *Davila* test. A different district court recognized this distinction, holding that where the gravamen of state common law claims was that the defendant had breached its fiduciary duties under ERISA, there was no complete preemption. There was no complete preemption because fiduciary claims are brought under Section 502(a)(2), not Section 502(a)(1)(B) as required under the *Davila* test. *Boyle v. SEIU Local 200 United Ben. Fund.*[53] I like the *Boyle* court's analysis as well because that court held that claims were preempted by ERISA even though there was no complete preemption. So, the court acknowledged the point I have made *ad nauseum* above that a lack of grounds for complete preemption does not mean claims are not preempted.

Although the *Rose* court may have been wrong in concluding that the first prong of the *Davila* test was met, it really didn't matter because the second prong of *Davila* was not met. There was, as a consequence, no complete preemption (and, the court seemed to say, there was also no preemption). That second prong of the *Davila* test is met only if the state law cause of action does not "arise independently of ERISA or the plan terms." Importantly in this regard, the court found that the plaintiff's allegations did not relate to the processing of any claim for benefits. As with *Dishman* above, even though the complained of conduct occurred in the course of administering a plan, the plaintiff's state law claims did not relate to the processing of a claim for benefits. Therefore, the plaintiff's state law claim that the TPA violated her right of privacy would exist regardless of the disposition of any claim for benefits processed by the TPA. And the state law cause of action for disclosure of the plaintiff's medical information would exist regardless of the TPA's case management undertaking and administration of the plan.

Because the second prong of *Davila* was not met, there was no complete preemption. The reader has surely picked up how frustrating I must find the next sentence of the court's opinion, in which the court said this also meant the claims were preempted: "Since the Court finds that the second prong of *Davila* is not satisfied, Plaintiff's privacy and unfair business practice cause of action are not preempted by ERISA."

Vaught v. Hartford Life & Accident Ins. Co. Relying on *Dishman*, a court held that invasion of privacy claims relating to an investigation under a long term disability plan were not preempted in *Vaught v. Hartford Life & Accident Ins. Co.*[54] 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

[53] 216 U.S. Dist. LEXIS 89810 (N.D. N.Y. 2016).
[54] 2011 U.S. Dist. Lexis 98945 (S.D Ohio 2011).

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 tortious conduct that amounts to an invasion of privacy would not 'relate to' the administration of the plan for purposes of pre-emption."

Prudence and Process. Prudence, remember, is about process. I asserted earlier that it is time for plan fiduciaries to start a process of considering, and beginning to address, privacy and security concerns as they relate to retirement, disability, and other plans not subject to HIPAA standards. We know that no foolproof processes can be implemented. But as a matter of "procedural prudence" it is probably time to start what may be an interminable and tedious process of considering, and continually improving, plan security and the protection of private information.

I'd argue that taking a few basic, and not especially painful, steps is the place to start, and may be adequate for the time being, at least in satisfying fiduciary's ERISA prudence obligations. The first and most important step is to focus on the security and privacy of information in the hands of plan vendors. After all, 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. In fact, 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.[55] The loans were taken from 58 participant accounts, but the recordkeeper reportedly restored the filched monies within five days.

And with respect to retirement plans, the compromise of a recordkeeper's system could lead to unauthorized benefit payments, such as withdrawals from 401(k) accounts. The importance to plan fiduciaries of having good processes in place is illustrated by *Foster v. PPG Indus.*,[56] where 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 employee's former spouse, who remained at the address, opened the mail one day and found new credentials for accessing the participant's 401(k) account online. She used a new password and the participant's social security number to create a user ID, password, answers to security questions, and beneficiary designation for the participant's account. The ex-wife changed the mailing address to her own P.O. box and requested a withdrawal of $4,000, to be directly deposited to a numbered account at a bank. The participant's former employer processed the request the next day. Since that worked, the ex-wife proceeded to empty the participant's account *in toto*, to the tune of in excess of $42,000.

The participant sued his former employer and the 401(k) plan, in an attempt to recover the monies stolen from his account. Interestingly, the Tenth Circuit concluded that the plan administrator was not required to reimburse the participant for the amount the ex-wife improperly

[55] https://chicago.suntimes.com/news/hackers-scam-2-6-million-from-city-retirement-accounts/ and http://www.pionline.com/article/20161017/PRINT/310179983/dc-plans-face-threats-to-crucial-data#.
[56] 593 F.3d 1226 (10th Cir. 2012).

took. The court reached this decision because the plan administrator properly disclosed to participants the plan's procedures for requesting distributions electronically, and closely followed those procedures.

As to the plan procedures, before the participant moved out of his marital residence, the former employer implemented an automated system to enable participants to access their 401(k) accounts, and notified participants how to use that system. The system used a combination of social security numbers and personal identification numbers to protect participants' accounts. The employer also notified participants that it would soon be introducing enhanced security measures to "address the increasing concern about possible identity theft and data privacy." These new measures included the use of unique user IDs, rather than social security numbers, and more complex password requirements.

So far, so good. But after the participant moved out of his former marital residence, without notifying his former employer of his change of address, the employer mailed information to the marital residence on how to establish a new user ID and password. The mail was marked "To Be Opened By Addressee Only." The problem was the ex-wife was still at the marital residence. She received the document and used the information in it, along with her ex-husband's social security number, to attempt to gain access to the participant's account online by resetting his password. In accordance with the employer's procedures, the employer processed the password reset request and sent it to the "permanent address on file," which was the marital residence where the ex-wife (and not the participant) was living. Now that she had the new password and her former husband's social security number, the ex-wife took the steps described earlier to wipe out the participant's account.

The important lesson for plan fiduciaries is that following a proper, and properly disclosed, process saved the plan administrator from being required to restore the participant's stolen monies.

There are some circumstances in which a plan's privacy and security initiatives may be unable to stop unauthorized access to retirement plan benefits. Sheer human depravity may prevail. In the summer of 2007, the U.S. Department of Justice announced that a retirement plan participant's spouse was sentenced to five years in prison for, among other things, making multiple unauthorized withdrawals from her husband's 401(k) account, totaling over $24,000, and over $16,000 in unauthorized loans.[57] The spouse made multiple calls to a 401(k) service center misrepresenting herself as her husband, and faxed supporting documentation to the service center in order to take hardship withdrawals, all without the participant's consent, knowledge, or authorization.

In discussing how liability might occur, I have largely focused on security breaches – that is, the unintended access to information by unauthorized persons. But we have also seen non-health plan examples of state law privacy claims that have been allowed to proceed where there has been no such breach. These cases have instead involved misuse of private information that has at least arguably been authorized by plan fiduciaries and involved intentional behavior. We

[57] https://www.justice.gov/usao-sdin/pr/evansville-woman-sentenced-federal-court-bankruptcy-and-wire-fraud-scheme.

saw this in both *Dishman* and *Rose* above, where the allegations concerned actions taken by plan vendors, not some unintended intruder into the plan's data.

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

- 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 that the virus was of a type that enabled the hacker to capture keystrokes when made by an authorized person, thereby 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 which was sent to a name different from the name on the account;
- Person hacking into database to gain access to more than 500,000 participants' PII due to failure of the plan (and administrators) to install security system updates;
- E-mail 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 more than 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, in many cases, 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.[58]

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. Press reports indicated that the UFCW Local 655 Food Employers Joint Pension Plan suffered a ransomware attack in July of 2016.[59] This security breach reportedly occurred when a hacker gained control

[58] "Privacy and Security Issues Affecting Employee Benefit Plans," U.S. Department of Labor Advisory Council on Employee Welfare and Pension Benefit Plans (Nov. 2011), p. 6.

[59] See, for example, https://www.prnewswire.com/news-releases/data-privacy-event-affects-ufcw-local-655-food-employers-joint-pension-plan-300360199.html; https://www.bna.com/ransomware-attack-hits-n57982082675/; and http://www.bnd.com/news/local/article115148918.html.

of one of the union's computer servers. The hacker demanded 3 bit coins 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.

Start with Vendors. Another reason to start the process of tightening a plan's privacy and security standards by focusing on plan vendors is that, curiously, it may be easier to take meaningful steps with vendors than it is to re-shape the internal processes at the sponsoring employer or other plan sponsor. After all, for most single employer plans benefit plan data is handled through a human resources or employee benefits department that is 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 that are 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 that there are non-IT driven steps one can take to improve privacy practices, the ability of a benefits department to take steps to improve IT security itself will typically depend on the cooperation and availability of other resources at the employer (or other plan sponsor).

So, what steps should fiduciaries take with respect to vendors? Here are some possibilities:

1. **Requests for Proposal**. In requests for proposal, fiduciaries may wish to inquire about the privacy and security standards vendors have in place. Fiduciaries may, in this regard, wish to ask for copies of "SOC" Reports. These are AICPA Service Organization Control Reports. A precursor of these reports were the SAS 70 reports.

   SOC Reports. There are three types of SOC Reports – SOC 1, SOC 2, and SOC 3. SOC Reports can be used by customers of service organizations, such as fiduciaries and plan sponsors of benefit plans, 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 controls at the vendor relevant to "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."

   There are two types of SOC 2 Reports. 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 in fact achieve the [vendor's] objectives. 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.

There is also a SOC 3 Report. As the AICPA describes it, a SOC 3 Report is "designed to meet the needs of users who need assurance about the controls at a service organization relevant to security, availability, processing integrity, confidentiality, or privacy, but do not have the need for or the knowledge necessary to make effective use of a SOC 2 Report." 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.

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, as well as the tests performed by the service auditor and the results of those tests, a SOC 2 Report is the right choice. In contrast, if customers do not have the need for, or the ability to understand, these details, a SOC 3 Report may be an appropriate choice.

Of interest, the AICPA has also developed a cybersecurity risk management reporting framework to enable organizations to communicate about the effectiveness of their cybersecurity risk management programs. In this connection, the AICPA has developed a new System and Organization Controls (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.

So, 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").[60]

FFIEC Cybersecurity Assessment Tool. For recordkeepers and other vendors affiliated with financial institutions, it may be worth asking for the results, if any, of their assessment of their vulnerability 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.[61]

[60] For more information, see the "Cybersecurity Considerations for Benefit Plans" report by the Department of Labor's Advisory Council on Employee Welfare and Pension Benefit Plans dated November 2016, page 13.

[61] The Federal Financial Institution Examination Council describes the Council as a "formal interagency body empowered to prescribe uniform principles, standards, and report form for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance

SEC Regulation S-P and FTC Red Flag Rules. In the case of vendors that are investment advisors (or brokers, dealers, transfer agents, or investment companies), SEC Regulation S-P requires the adoption of policies and procedures reasonably designed to meet various objectives relating to security and confidentiality. And certain financial institutions are required by the Federal Trade Commission "Red Flag" rules to have and implement a written identity theft program.[62] For financial institutions and others subject to the SEC regulation or FTC Red Flag rules, it may therefore be worth asking about their compliance with those requirements.

For an example of an SEC enforcement action relating to cybersecurity and the failure to meet the requirements of Regulation S-P, see the Administrative Proceeding order in the matter of R.T. Jones Capital Equities Management, Inc.[63] 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 as a result, between 2011 and 2014 a then-employee impermissibly accessed and transferred to his personal server data relating to approximately 730,000 accounts, which data was ultimately hacked by third parties.

2. **Vendor Contracts.** When entering into agreements with new vendors, it may be wise to consider incorporating into the contract elements of a typical HIPAA business associate agreement. These might include rules as to who the vendor can communicate with (for example, 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 HHS-approved technology standards for data in motion, including appropriate 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 in the event of a breach a violation of the law.

In new vendor contracts, fiduciaries may also wish to require vendor representations, and indemnification protection, with respect to 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 statutes

---

Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Consumer Financial Protection Bureau (CFPB) and to make recommendations to promote uniformity in the supervision of financial institutions."

[62] https://www.ftc.gov/tips-advice/business-center/guidance/fighting-identity-theft-red-flags-rule-how-guide-business.

[63] https://www.sec.gov/news/pressrelease/2016-112.html

mentioned in the text associated with footnotes 22 through 25 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.

As to 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 that it has met these standards.

For a superb, and more comprehensive, list of considerations with respect to vendor contract provisions relating to privacy and security protection, see "Fiduciary Issues and Data Privacy: Is Your Plan Data Really Safe?," PowerPoint presentation by Ann Killilea and Andrew C. Liazos, March 23, 2016.[64]

3. **Existing Vendors**. Though it may be more difficult, fiduciaries may wish to begin taking steps with existing vendors like those described above for new vendors. So, for example, it may make sense to begin asking existing vendors for SOC Reports, and begin incorporating into agreements the contractual provisions described above upon the renewal, extension, or amendment of existing agreements.

4. **SAFETY Act**. Plan sponsors may wish to consider retaining vendors using technology that has received a Support Anti-Terrorism by Fostering Effective Technologies Act of 2002 ("SAFETY Act") "designation" or "certification." For a suggestion that compliance with SAFETY Act standards may, however, not be cost-effective, see the "Cybersecurity Considerations for Benefit Plans" report of the Department of Labor's Advisory Council on Employee Welfare and Pension Benefit Plans, November 2016 report, page 11.

Internal Steps. Although I have expressed some cynicism about the ability of an HR or benefits department to quickly change an employer or other plan sponsor's IT security practices and procedures, a reasonable and achievable model for improving internal security and privacy controls may be the plan sponsor's existing HIPAA privacy and security procedures. I do not mean to suggest that all of the standards set forth in those procedures need to be applied with respect to retirement or other non-health plan data, but one might consider whether application of a stripped down version of those processes to personally identifiable information might be appropriate. And something more robust might make sense with respect to information that involves an individual's health or other information an employer could be accused of misusing, for example to fire an employee. The obvious example would be information relating to disability benefit claims. Being able to show 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.

[64] available at https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwjZvJy39vrXAhWp1IMKHb-NBKcQFggpMAA&url=https%3A%2F%2Fwww.employeebenefitsblog.com%2Fwp-content%2Fuploads%2Fsites%2F23%2F2016%2F04%2FMicrosoft-PowerPoint-Fiduciary-Issues-and-Data-Privacy-Killilea-Liazos-3-23-16.pdf&usg=AOvVaw2ZdY-AfA-8U52gKw88dr-8.

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.

Compliance with State Statutes. The suggestions above relate primarily to attempt to satisfy 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 state-by-state listing of statutes found in footnotes 22 through 25 associated with the text above under the heading "State Law."

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 any existing coverage 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.

Other Steps. For further suggestions about possible approaches for increasing privacy and security protections, including at the employer or other plan sponsor level (as opposed to at the vendor level), fiduciaries may wish to refer to the report by the Department of Labor's Advisory Council on Employee Welfare and Pension Benefit Plans from November 2016, entitled "Cybersecurity Considerations for Benefits Plans." This 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 entitled "Small Business Information Security: The Fundamentals," dated November 2016.[65]

[65] This is available at http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf.