Nationwide®
is on your side

The Advanced Consulting Group

White paper

Cyber and data security issues for ERISA-covered retirement plans

Chuck Rolph, JD, MSFS, CFP®, AIF®, CEBS, CPC, CPFA, TGPC, CLU®, ChFC®, RICP
Director, Advanced Consulting Group

I. Background

In today's modern world, we are all affected by the internet and technology. Along with the technological advances that make our lives as consumers and members of society easier come risks, such as the risks of identity theft and financial crimes. Plan sponsors, fiduciaries, and their advisors need to be aware of the liability they face in accordance with their obligation to protect the integrity of the data of the plans that they serve from identity theft and financial crimes. The purpose of this paper is to provide that audience with information concerning their responsibilities and potential liabilities under the Employee Retirement Income Security Act of 1974, as amended ("ERISA") with respect to cyber and data security issues associated with ERISA-covered retirement plans.

II. General fiduciary responsibilities and duties under ERISA

2.1. No explicit provision in ERISA dealing with cyber and data security. There is no explicit provision in ERISA that sets standards for plan fiduciaries in terms of their obligations for cyber and data security. Because there is no such explicit provision, we will review the general affirmative duties of an ERISA fiduciary in subsection 2.2.

2.2. General affirmative duties of an ERISA fiduciary. Also, sometimes referred to as the "affirmative duties rule," ERISA section 404(a) imposes affirmative duties on a fiduciary of the plan. Specifically, ERISA section 404(a)(1) requires a fiduciary to discharge his or her duties with respect to a plan solely in the interest of the participants and beneficiaries and — (A) for the exclusive purpose of: (i) providing benefits to participants and their beneficiaries; and (ii) defraying reasonable expenses of administering the plan; (B) with the care, skill, prudence, and diligence under the circumstances then prevailing that a prudent person acting in a like capacity and familiar with such matters would use in the conduct of an enterprise of a like character and with like aims; (C) by diversifying the investments of the plan so as to minimize the risk of large losses, unless under the circumstances it is clearly prudent not to do so; and (D) in accordance with the documents and instruments governing the plan insofar as such documents and instruments are consistent with the provisions of Titles I and IV of ERISA.

2.2.1. Of the enumerated affirmative fiduciary duties, the two that would most likely be asserted to support a position that ERISA encompasses a fiduciary duty involving cyber and data security would be the duty of prudence and the duty to administer the plan in accordance with the documents and instruments governing the plan.

2.2.2. The duty to discharge one's fiduciary duty with the care, skill, prudence, and diligence under the circumstances then prevailing that a prudent person acting in a

like capacity and familiar with such matters would use in the conduct of an enterprise of a like character and with like aims potentially could be argued to encompass cyber and data security. A participant who suffers adverse financial consequences as a result of a data breach in the plan of which he or she participates would most likely allege a breach of fiduciary duty in terms of a lack of care, skill, prudence, and diligence by the fiduciary in charge of the plan's data in an effort to obtain a monetary recovery.

2.2.3. Most plan and trust documents typically do not include provisions that specifically address data security. These kinds of provisions may be found in procedures manuals that the fiduciaries of the plan would adopt in order to set guidelines for the operation and administration of the plan. Once written guidelines or procedures pertaining to the operation and administration of the plan are adopted by a fiduciary, failure to follow them could be alleged to be a breach of fiduciary duty. Thus, a participant who incurred a financial loss as a result of a data breach might (through his or her attorney) seek to conduct discovery to see whether or not the plan fiduciaries had adopted written procedures associated with cyber and data security. If such written procedures had been adopted, the next inquiry would be to see whether the procedures had been followed. If the procedures had not been followed, then an allegation of a breach of fiduciary duty could be made by the aggrieved participant. If the plan fiduciaries had not adopted written procedures for plan administration that encompassed cyber and data security, an aggrieved participant could (through his or her attorney) allege a breach of fiduciary duty for not having adopted such procedures.

2.3. If there is a breach of fiduciary duty that does not involve a prohibited transaction, then certain ERISA sections apply that detail the liability of a fiduciary for a fiduciary breach.

2.3.1. ERISA section 409(a) provides that a fiduciary is personally liable to restore to the plan any losses resulting from a breach of fiduciary duty. A lawsuit may be brought by affected participants for equitable relief in conjunction with the breach of fiduciary duty under ERISA section 502(a).

2.3.2. ERISA section 501 sets out criminal penalties for a willful violation of Title I of ERISA — up to $100,000 in fines and up to 10 years in prison. ERISA section 502(a) allows participants and the DOL to file lawsuits against the fiduciary in order to enjoin proscribed conduct and/or provide for equitable relief.

2.3.3. Should the U.S. Department of Labor ("DOL") recover any money from a fiduciary either as a result of a settlement or a court order, ERISA section 502(l) provides for a civil penalty of 20% of the "applicable recovery amount" from the fiduciary. This civil penalty under section 502(l) is reduced by both the administrative civil penalty imposed on a person and any excise taxes paid pursuant to Code Section 4975.

2.3.4. ERISA section 502(i) imposes an "administrative civil penalty" for violations by plans that are not subject to Code Section 4975, including welfare plans or health plans funded through a VEBA trust. This administrative civil penalty is five percent of the amount involved in the transaction, rising to 100 percent if the prohibited transaction is not corrected within 90 days after a final order is issued by the DOL.

2.4. Fiduciary legal standard. As noted by the court in the case of *Donovan v. Bierwith*[1], "... the fiduciary obligations of the trustees to the participants and beneficiaries of the plan are those of trustees of an express trust — the highest known to the law." In interpreting this fiduciary legal standard as it might apply to a fiduciary's duty with respect to cyber and data security, the case of *DeBruyne v. Equitable Life Assurance Society of the United States*[2] may be instructive. In *DeBruyne*, the plan trustees were found not to have violated the fiduciary duties established by ERISA by failing to anticipate the stock market crash of 1987. The *DeBruyne* court famously declared that the fiduciary duty of care requires prudence, not prescience.

2.4.1. The takeaways for plan fiduciaries from the two aforementioned cases are that they, as fiduciaries: (i) have a duty to their participants and beneficiaries to act responsibly and with prudence in safeguarding the plan's data; and (ii) are not absolute guarantors of data security — they are only duty bound to act prudently, diligently, and with the expertise of a prudent expert.

2.4.2. From the case law on the subject of a fiduciary's prudence, we can find cases that deal with a fiduciary's selection of plan investments. This genre of cases is instructive in terms of discerning the steps a fiduciary must take to satisfy his or her obligation to act in a prudent manner and the extent to which the fiduciary may be held liable for the ultimate outcome of a transaction. In the case of *Donovan v. Mazzola*, the test of prudence was described

in fairly procedural terms, as "whether the individual trustees, at the time they engaged in the challenged transactions, employed the appropriate methods to investigate the merits of the investment and to structure the investment."[3] The case of *Anderson v. Mortell*,[4] is an example of the principle that following a prudent fiduciary process when selecting investments or carrying out other fiduciary duties is more important than the actual outcome of the fiduciary's decisions. In that case, the court found that the duty of the fiduciary is to conduct a prudent, independent investigation, and not to achieve "the highest possible price" in a sale of plan assets.

2.4.3. The takeaway for a fiduciary concerned with his or her duties and potential liability in connection with cyber and data security of plan data is that the fiduciary must have established and followed a prudent process for securing the plan's and its participants' data, both electronically and otherwise. From a reading of the cases involving fiduciary duty in the context of investment selection, we can extrapolate that a fiduciary most likely would not be held liable for a cyber or hard copy data breach if, despite the best efforts of the affected fiduciary who established a prudent process and procedures for handling such data, a breach occurred. Once such processes and procedures are established, the affected fiduciaries must follow them if they hope to limit liability for a cyber or hard copy data breach. If the affected plan fiduciary did not have in place a framework of policies and procedures (separate and apart from any language contained in the plan and trust documents) for addressing the security of electronic and hard copy data, it would be extremely hard to make the case that such fiduciary acted with the necessary level of care and prudence that would be sufficient to protect the fiduciary from liability in the event of a data breach.

2.4.4. As part of establishing prudent processes and procedures for the protection of electronic and hard copy plan and participant data, the fiduciary should consider the following elements:

A. Selection and monitoring of service providers to make sure that they have established practices and procedures that emphasize data security;

B. Written contracts with service providers to include provisions that make it the responsibility of the service provider to maintain data security standards that are consistent with industry best practices;

C. Operate the plan and transactions with the plan's data on a strictly "need to know" basis; i.e., only those employees and outside service providers who are performing specified administrative functions should have access to plan and participant data, and only to the extent necessary to do their respective jobs;

D. The plan fiduciaries should consider employing outside professionals to assist with the establishment of processes and procedures to safeguard plan and participant data; and

E. In order to objectively establish that the established practices and procedures with respect to plan and participant data are being followed, the plan fiduciaries may wish to employ the services of an outside consulting firm to assess the effectiveness of its practices and procedures. Any deficiencies reported by the outside consultant should be immediately remediated.

III. Cyber and data security - summary of the existing legal framework[5]

3.1. As noted in the 2011 Advisory Council on Employee Welfare and Pension Benefit Plans ("Council") report, there continues to be no comprehensive federal law governing cybersecurity for benefit plan service providers. There are laws that govern the financial industry's use of financial information, such as the Fair Credit Reporting Act, Gramm-Leach-Bliley Act, and the Fair and Accurate Credit Transactions Act. These laws, however, do not apply specifically to benefit plans or the sensitive individual data held in conjunction with those plans. Furthermore, the guidance from the Council addresses neither the scope of ERISA fiduciary obligations regarding cybersecurity, nor whether ERISA preempts state data breach laws. Even though the focus of this paper is on retirement plans, the discussion in this section encompasses employee welfare benefit plans, as well. Thus, the term "benefit plans" refers to both employee pension benefit plans and employee welfare benefit plans.

3.2. Benefit plans typically maintain data elements that can make up Personally Identifiable Information ("PII") and Protected Health Information ("PHI").

3.2.1. The Office of Management and Budget ("OMB") defines PII as: "Information which can be used to distinguish or trace an

individual's identity, such as his or her 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."[6]

3.2.2. PHI is akin to Individually Identifiable Health Information, defined under HIPAA[7] as: "Information that is a subset of health information, including demographic information collected from an individual, and: (1) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (i) that identifies the individual; or (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the individual. "

3.3. Many states have laws that address the protection of PII and PHI in some form but, like federal laws, these laws generally apply to health plans, and not to other welfare benefit plans or to pension plans. Existing legislation provides some guidance for how sponsors might approach the problem. Under HIPAA, health plan sponsors already manage their plans in accordance with data privacy and security rules. Health plan sponsors enter into business associate agreements with TPAs and other service providers. Business associate agreements establish each party's obligations under HIPAA in connection with the plan's HIPAA-protected information.

3.4. In addition to HIPAA, health plan sponsors might also reference state data breach notification laws and cyber liability insurance in business associate agreements. Several witnesses referenced these business associate agreements as examples of a potential approach that could be used in the broader benefit plan universe. Business associate agreements, HIPAA and the myriad of state laws provide a starting framework for guiding other types of benefit plans, their sponsors and fiduciaries in considering how to approach cybersecurity issues and handling PII.[8]

3.5. The 2016 Advisory Council report focuses on three key areas of emphasis in the cyber and data security arena to help plan fiduciaries and their service providers.

3.5.1. Establish a strategy. First-of-all, identify the data (e.g., how it is accessed, shared, stored, controlled, transmitted, secured and maintained). Next, consider following existing security frameworks available through organizations such as the National Institute of Standards and Technology ("NIST"), Health Information Trust Alliance ("HITRUST"), the Support Anti-terrorism by Fostering Effective Technologies Act of 2002 ("SAFETY Act"), and industry-based initiatives. Thirdly, establish process considerations (e.g., protocols and policies covering testing, updating, reporting, training, data retention, third party risks, etc.). Then, each plan fiduciary and service provider should develop a customized strategy for implementing the security measures they develop by taking into account resources, integration, cost, cyber insurance, etc. In order to create a strategy that is appropriate for the plan involved, it is necessary to strike the right balance based on size, complexity and overall risk exposure. In so doing, consider applicable state and federal laws.

3.5.2. Contracts with service providers. In any written contract for services with a service provider to the plan, start by defining the security obligations of the service provider in its dealings with the plan. Next, identify reporting and monitoring responsibilities of the service provider to the responsible plan fiduciary who hired and then monitors the service provider's conduct of its services. Thirdly, plan fiduciaries should conduct periodic risk assessments. The responsible plan fiduciary of each plan has a responsibility to establish due diligence standards for vetting service providers based on the sensitivity of data being shared in an effort to prevent data breaches. Remember, sensitive data should only be shared on a need-to-know basis. Finally, in deciding whether or not to hire a particular service provider, consider whether the service provider has a cyber security program, how data is encrypted, liability for breaches, etc.

3.5.3. Insurance. Understand overall insurance programs covering plans and service providers. Evaluate whether cyber insurance has a role in a cyber risk management strategy. Consider the need for both first and third party coverage.

3.6. At the time of the report (November 2016), no comprehensive cybersecurity protocol for retirement plan administration existed at the federal level. The Council has provided suggested materials for plan sponsors, fiduciaries and service providers to utilize when developing a cybersecurity strategy and program.

IV. IRS Publication 4557. Safeguarding Taxpayer Data — A Guide for Your Business

Although this publication from the IRS is directed primarily to those who are in the business of preparing tax returns, it is extremely useful for plan fiduciaries in terms of providing practical resources for establishing and maintaining an electronic and hard copy data security program. The contents of the publication may be summarized as follows:

- Protect your clients; protect yourself
  - Take basic security steps
  - Use security software
  - Create strong passwords
  - Secure wireless networks
  - Protect stored client data

- Be on guard
  - Spot data theft
  - Monitor electronic filing identification numbers and preparer tax identification numbers
  - Recognize phishing scams
  - Guard against phishing emails
  - Be safe on the internet

- Report and respond
  - Report data loss to IRS/states
  - Respond and recover from a data loss

- Comply with the Federal Trade Commission ("FTC") safeguards rule
  - Understand the FTC safeguards rule
  - Comply with the FTC safeguards rule
  - Use the safeguards rule checklist
  - Employee management and training
  - Information systems
  - Detecting and managing system failures

V. Impact of state laws on plan and participant data breaches

5.1. Each state has its own unique law in place that covers a data breach and the requirements for the security of specific information described in the law. Following are the elements that a fiduciary would consider in analyzing the effects of the applicable state law on the fiduciary and/or the plan:

5.1.1. Applicability of the law and definition of what constitutes a data breach and, thus, a reportable offense. Most state laws seem to define their coverage in terms of individuals and businesses who possess and work with confidential data. The issue, then, is whether the law in question specifically covers a plan and/or fiduciaries of the plan; or, whether there is an inference of such coverage. Advice from local legal counsel would be required to properly answer this question.

5.1.2. Notification requirements. The applicable state law will specify the group of individuals and government agencies (i.e., regulators) that must be notified in the event of a data breach. This section of the applicable law will also likely include the acceptable means by which such notification can be made.

5.1.3. Penalties. Naturally, the applicable law may also specify the penalties for a violation of the law.

5.1.4. Special considerations unique to the state in question.

5.2. ERISA preemption. Any discussion of a state law on the subject of data breaches as possibly applying to a plan covered by ERISA should take into account the ERISA preemption clause, as found in ERISA 514(a), and the ERISA civil enforcement provision, as found in ERISA 502(a).

5.2.1. ERISA 514(a) provides that: Except as provided in subsection (b) of this section [no relief from state laws involving insurance, banking, and securities], the provisions of titles I and IV shall supersede any and all State laws insofar as they may now or hereafter relate to any employee benefit plan described in section 4(a) [pension and welfare benefit plans] and not exempt under section 4(b) [government and non-electing church plans].

5.2.2. ERISA 502(a) is the civil enforcement provision and authorizes a participant or beneficiary to bring a civil action for: (i) the relief provided for in ERISA 502(c) [plan administrator's failure to provide information]; or (ii) to recover benefits due to him or her under the terms of his plan, to enforce his or her rights under the terms of the plan, or to clarify his or her rights to future benefits under the terms of the plan.

5.3. *In Re Anthem, Inc. Data Breach Litigation*,[9] hereinafter referred to as the *Anthem* case. The case ultimately settled, effective as of August 15, 2018. It is discussed herein because of the rulings made on

the issue of preemption of state law claims against an employee welfare benefit plan subject to ERISA.

5.3.1. The essence of the *Anthem* case is about preemption and the interpretation of ERISA 502(a) by the court to allow the defendants to remove the case from a state court in New York, where it was filed, to the federal district court system. The case involved data breaches of personal health information ("PHI"). One of the allegations made by the plaintiffs in the lawsuit was that Anthem (the defendant) violated the New York state law on data breaches and, as a result, the plaintiffs brought their action in New York state court.

5.3.2. On April 27, 2015, Defendants removed this action to the United States District Court for the Eastern District of New York. Defendants provided two independent bases for federal subject matter jurisdiction: (i) federal question jurisdiction under ERISA; and (ii) federal question jurisdiction under the Health Insurance Portability and Accountability Act ("HIPAA")[10]. On October 13, 2015, the Judicial Panel on Multidistrict Litigation transferred the case (a putative class action) from the Eastern District of New York to the judge in the Northern District of California. That is why the case is cited as coming from the Northern District of California, even though it was originally filed in New York state court. The Court declined to address whether federal question jurisdiction exists under HIPAA."5.3.3. A suit may be removed from state court to federal court only if the federal court would have had subject matter jurisdiction over the case in the first instance.[11] In civil cases, subject matter jurisdiction is generally conferred upon federal district courts either through diversity jurisdiction [28 U.S.C. sec. 1332], or federal question jurisdiction [28 U.S.C. sec. 1331]."[12] If it appears at any time before final judgment that the federal court lacks subject matter jurisdiction, the federal court must remand the action to state court [28 U.S.C. sec. 1447(c)]. In *Anthem*, the court found that Plaintiffs' claims are completely preempted by ERISA's civil enforcement provision [ERISA 502(a)] and that, as a result, the federal district court (not the New York state court) has subject matter jurisdiction over this action.

5.3.4. The court described the interplay between ERISA 502(a) and ERISA 514(a) in the following manner. One form of ERISA preemption is "complete preemption" under ERISA 502(a), which provides that a civil enforcement action may be brought by a participant or beneficiary: (i) to recover benefits due to him or her under the terms of the plan; (ii) to enforce his or her rights under the terms of the plan; or (iii) to clarify his rights to future benefits under the terms of the plan. The other form of ERISA preemption is that found under ERISA 514(a). Pursuant to this provision, "any state-law cause of action that duplicates, supplements, or supplants the ERISA civil enforcement remedy" is preempted because it "conflicts with the clear congressional intent to make the ERISA remedy exclusive."[13]

5.3.5. *Davila* applies a two-pronged test for determining whether an action filed in state court is preempted. Specifically, a state law cause of action is completely preempted and therefore removable to federal court "if (1) an individual, at some point in time, could have brought [the] claim under ERISA 502(a) (1)(B), and (2) where there is no other independent legal duty that is implicated by a defendant's actions."[14] The court recognized that because *Davila's* two-pronged test is stated "in the conjunctive," a state law cause of action is preempted and removal is proper only if both prongs of the test are satisfied. Factually, the court found that the plaintiffs could have brought their action under ERISA 502(a). As explained in *Davila*, ERISA preemption applies "if an individual, at some point in time, could have brought his claim under ERISA 502(a)(1)(B)."[15] As to the second *Davila* prong, plaintiffs argued that defendants had an independent legal duty to protect plaintiffs' privacy pursuant to state law. Plaintiffs argued that their ERISA plan coverage and benefits do not include and have not been shown to include privacy rights. The court factually observed that the plaintiffs' contentions were belied by language in the affected plan's summary plan description (a/k/a, Benefits Handbook) wherein it was stated under a section titled "State Notice of Privacy Statutes,": … "we [defendants] must follow state laws that are more strict than the federal HIPAA privacy law."[16] The Benefits Handbook proceeds to then "explain[] [Plaintiffs'] rights and [Defendants'] legal duties under state law." *Id.* As the U.S. Supreme Court has held, duties under state law are not independent of ERISA when "interpretation of the terms of respondents' benefit plans forms an essential part of [respondents'] claim." *Davila*, 543 U.S. at 213. In *Marin General Hospital v. Modesto & Empire General Traction Company*[17], the Ninth Circuit further held that state law legal duties are not independent of ERISA if they are "based on an obligation under an ERISA plan" and if "they would [not] exist [if the] ERISA plan" did not exist.

5.3.6. In the instant case (i.e., *Anthem*), the court found that defendants' duty to comply with state privacy laws clearly represents an obligation under plaintiffs' ERISA plan. In addition, the court stated that defendants would not have been under such an obligation but for the fact that plaintiffs were members of an ERISA plan that was administered by defendants. Thus, defendants did not have an independent legal duty to protect plaintiffs' privacy pursuant to state law. Because the court found that the duty to protect plaintiffs' privacy arose under an ERISA plan, state law on privacy was, in effect, preempted by ERISA.

5.3.7. The bottom line of the *Anthem* case is that, under the right set of facts and circumstances, a strong argument can be made that state data breach laws are preempted, when such laws are attempted to be applied to an ERISA plan.

5.4. *In Re: Premera Blue Cross Customer Data Security Breach Litigation*[18].

5.4.1. The *Premera* case involved a data breach by a Blue Cross subsidiary in the context of a health plan subject to ERISA. The facts of the case are complex and, due to the space limitations of this paper, will not be discussed. We will, instead, examine the court's analysis of ERISA 502(a)(1)(B), as it pertains to the question of preemption of state law by ERISA.

5.4.2. The court took notice of the two-pronged test for complete preemption referenced in the *Davila* case, as discussed in paragraph 5.3.5, above. In response to the preemption argument, the plaintiffs in the case (who were seeking state court jurisdiction of the case) made the following two arguments: (i) data protection is not a "benefit" as that term is used in ERISA and thus plaintiffs could not bring a claim under ERISA 502(a); and (ii) even if data protection is an ERISA benefit, complete preemption is not applicable because plaintiffs allege that Premera's duty to protect plaintiffs' sensitive information arises independently from the ERISA plan documents.

5.4.3. The court agreed with the plaintiffs that data protection or security is not a benefit under ERISA 502(a). The court disagreed, however, that all three types of claims under ERISA 502(a)(1)(B) must involve a "benefit." ERISA 502(a)(1)(B) provides for three types of claims: (i) to recover benefits due under the plan; (ii) to enforce rights under the terms of the plan; or (iii) to clarify rights to future benefits under the terms of the plan. Citing *Davila*, the court noted that the first and third types of claims involve benefits under the ERISA plan. The second type of claim, however, more broadly allows a participant or beneficiary to enforce his or her rights under the plan, without reference to "benefits." The court concluded that if Congress intended the second type of claim to only involve the enforcement of benefits, it could easily have stated as much, like it did with the first and third types of claims.

5.4.4. Next, the court focused on the second prong of the *Davila* test; namely, that there is no other independent legal duty that is implicated by a defendant's actions. First, the court noted that Premera was required to protect plaintiffs' sensitive information under state law, HIPAA, and industry standards, regardless of what is contained in the health insurance contracts. The court found that plaintiffs' allegations were sufficient to show that their claims are not solely and entirely dependent on the ERISA plan. Then, the court concluded 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. Moreover, plaintiffs have sufficiently alleged an independent legal duty separate from the ERISA plan that has been implicated by Premera's alleged actions. Thus, complete preemption under ERISA does not apply.

5.4.5. The takeaway from the *Premera* case is that, like *Anthem*, facts and circumstances do matter. The two-prong test of the *Davila* case [see paragraph 5.3.5] is what was used in *Anthem* and in *Premera* to determine whether preemption applies. If both prongs of the test are not met, then the party seeking to use the preemption tool to remove the case to federal court will not prevail.

5.5. In this section V, we explored the relationship of state laws on privacy and data breaches to plans covered by ERISA and the individuals who participate in them. We were not able to discern any hard and fast rule regarding whether or not ERISA would preempt a state law on privacy and data breaches when the data breach affected participant data related to an employee benefit plan. It comes down to whether or not both parts of the two-pronged test announced in the *Davila* case are met.

VI. Conclusion

The responsible plan fiduciaries and the service providers they hire should consider the implementation of common-sense practical measures to safeguard data. Because most plan fiduciaries are not experts in the field of data security, they should consider hiring consultants with the necessary expertise to design and implement a complete data security program for the affected plan and its participants. Examples of common-sense practical measures to safeguard data include, but are not limited to the following:

- Managing logins, to include passwords, two-factor authentication of someone trying to access an account, etc.
- Establish procedures to validate electronic and digital signatures.
- Develop procedures for securing the plan and participant data, as was discussed above. This is an especially important item to be included in any contract with a service provider to the plan.
- Training of employees who handle plan and participant data so that they are aware of the procedures regarding data security established by the plan fiduciary.
- Supervision and monitoring by an independent fiduciary of the plan (i.e., one who is not involved in the day-to-day administration of the affected plan).

[1] 680 F. 2d, 263, 272, n.8 (2d Cir. 1982).
[2] 720 F. Supp. 1342 (N.D. Ill. 1989), affd. 920 F.2d 457 (7th Cir. 1990).
[3] 716 F.2d at 1232.
[4] 722 F. Supp. 462, 11 EBC 1890 (N.D. Ill. 1989).
[5] Taken from the Advisory Council on Employee Welfare and Pension Benefit Plans Report to Thomas E. Perez, U.S. Secretary of Labor, November 2016.
[6] Office of Management and Budget Memorandum M-07-16 "Safeguarding Against and Responding to the Breach of Personally Identifiable Information."
[7] Section 1171 of Part C of Subtitle F of Public Law 104-191 (August 21, 1996: Health Insurance Portability and Accountability Act of 1996: Administrative Simplification and 45 CFR (Code of Federal Regulations) 160.103.
[8] Christensen, Lisa; "Cybersecurity and Employee Benefit Plan Fiduciary Duties: Going Beyond HIPAA" April 26, 2016 posted in Cybersecurity, Employee Benefits published by the Labor and Employment attorneys of Bond, Schoeneck and King.
[9] U.S. District Court, N.D. California, (Nov. 24, 2015).
[10] 42 U.S.C. sec. 1320d et seq.
[11] 28 U.S.C. sec. 1441(a); see *Caterpillar Inc. v. Williams*, 482 U.S. 386, 392 (1987). "Only state-court actions that originally could have been filed in federal court may be removed to federal court by the defendant."
[12] *Peralta v. Hispanic Bus., Inc.*, 419 F.3d 1064, 1068 (9th Cir. 2005).
[13] *Aetna Health Inc. v. Davila*, 542 U.S. 200 at 209 (2004). Hereinafter referred to as *Davila.*
[14] *Davila*, 542 U.S. at 210.
[15] *Id.*
[16] Benefits Handbook at 43.
[17] 581 F.3d at 950 (9th Cir. 2009). Hereinafter referred to as *Marin General Hospital*.
[18] U.S. Dist. Ct., D. Oregon, (Feb. 9, 2017). Hereinafter referred to as the *Premera* case.