NORTH CAROLINA LAW REVIEW

Volume 99 | Number 3 Article 6

3-1-2021

Preemption Problem: Does ERISA Preempt the California Consumer Privacy Act?

Katherine Q. Morrow

Preemption Problem: Does ERISA Preempt the California Consumer Privacy Act?*

Congress passed the Employee Retirement Income Security Act of 1974 ("ERISA") to ensure that when private employers establish benefit plans for their employees, they keep their promise to provide those benefits. This comprehensive regulatory scheme governs benefits administration, establishes plan reporting requirements, and defines fiduciary duties for those involved in plan administration and decision-making. But ERISA is silent on a key issue affecting plan participants and sponsors today—data privacy and security.

The California Consumer Privacy Act ("CCPA"), enacted in 2018 and effective beginning January 1, 2020, represents the most comprehensive data privacy law in the United States. If the CCPA applies to ERISA plans, it will force plan sponsors and administrators to strengthen their data security protocols, increasing participants' data security and consumer rights while also increasing plan administration costs. But whether the CCPA applies to ERISA plans remains an open question.

ERISA may preempt the CCPA if a court were to find that the CCPA impermissibly interferes with the administration of ERISA plan benefits. If ERISA preempts the entire CCPA, plans would be exempted from compliance with generally applicable state data privacy laws that would otherwise improve plan security and therefore benefit plan participants. This Comment argues that because ERISA does not create an explicit duty for plans to reasonably safeguard data and the CCPA applies generally, courts should allow for provisions of the law that are not directly connected with employee benefits administration to escape preemption.

INTRODUCTION

As of June 2020, 401(k) retirement plans in the United States held an estimated $6.3 trillion in assets.[1] As work and communications become increasingly virtual, these retirement assets become more vulnerable to data breach and cyber fraud.[2] In the event of a cyberattack or data breach, plan beneficiaries may potentially hold the plan administrators and fiduciaries liable, but the applicable law and the extent of its protection remains unsettled.[3]

The Employee Retirement Income Security Act of 1974 ("ERISA")[4] regulates employer-sponsored pension and healthcare plans. Congress passed ERISA to promote these plans and ensure that policyholders receive full benefits even if their employer becomes insolvent.[5] One of ERISA's primary

1. *Frequently Asked Questions About 401(k) Plan Research*, INV. CO. INST., https://www.ici.org/policy/retirement/plan/401k/faqs_401k [https://perma.cc/7V2F-4TA9] (last updated Oct. 2020).

2. *See* Jeffrey D. Mamorsky, *Insight: Coping with 401(k) Cyberattacks and Fraudulent Plan Distributions*, BLOOMBERG L. (June 18, 2020, 4:01 AM), https://news.bloomberglaw.com/employee-benefits/insight-coping-with-401k-cyberattacks-and-fraudulent-plan-distributions [https://perma.cc/UPR5-KQKK].

3. *See* Gregg Moran, *Breaches Within Breaches: The Crossroads of ERISA Fiduciary Responsibilities and Data Security*, 73 UNIV. MIAMI L. REV. 483, 485–87 (2019).

4. Pub. L. No. 93-406, 88 Stat. 829 (codified as amended in scattered sections of 26 U.S.C. and 29 U.S.C.).

5. *See id.* § 2, 88 Stat. at 833 (codified as amended at 29 U.S.C. § 1001(c)). ERISA was passed partly in response to large businesses failing and being unable to pay pension benefits to their employees because the plans were not adequately funded. Robert A. Cohen, Note, *Understanding Preemption Removal Under ERISA § 502*, 72 N.Y.U. L. REV. 578, 588 (1997). Congress wanted to ensure

goals was to facilitate uniform administration of pension and healthcare plans[6] nationwide, and it contains two preemption[7] provisions to achieve this goal.[8] Generally, ERISA may preempt a state law if it (1) conflicts with ERISA's civil enforcement scheme[9] or (2) if the state law "relates to" an ERISA plan such that it would interfere with the uniform administration of the plan.[10] ERISA's broad preemption standard allows for covered plans to avoid potential liability under state laws that impact the administration of the plan's benefits; however, the Supreme Court's inconsistent interpretation of the ERISA preemption standard makes it notoriously difficult to predict whether preemption applies in a given scenario.

When Congress enacted ERISA in 1974, data privacy and data security were not issues on the national radar. At that time, the most advanced piece of related technology in ERISA administration was the fax machine, and plans mailed communications and distributed disbursements by check.[11] Today, plan participants most frequently interact with their plans online, transmitting personally identifiable information ("PII"), which puts participants' information at risk in the event of a data breach.[12] ERISA's text does not address plan participants' rights to a cause of action in the event of a data breach nor does it address participants' data privacy rights. Although several federal

that older workers who planned to receive retirement funds from pension plans would actually receive those funds. *Id.*

6. *See* § 4, 88 Stat. at 839 (codified as amended at 29 U.S.C. § 1003(a)). ERISA generally covers any employee benefit plan that is established or maintained "by any employer engaged in commerce or in any industry or activity affecting commerce" or "by any employee organization or organizations representing employees engaged in commerce or in any industry or activity affecting commerce" or "by both." *Id.* Pension plans are plans that provide retirement income to workers, while welfare plans provide other benefits such as healthcare, disability, death, or unemployment benefits to workers, but not retirement income. Cohen, *supra* note 5, at 589.

7. Preemption occurs when a state law is displaced by a federal statute. *See* Caleb Nelson, *Preemption*, 86 VA. L. REV. 225, 225–26 (2000). The Supreme Court has developed a framework to analyze preemption. *Id.* at 226. A federal law may preempt state law in three ways by: (1) including a preemption clause expressly withdrawing power from the states (express preemption), (2) regulating an area so completely that it "withdraws state lawmaking power over that field" (field preemption), or (3) conflicting with the state law (conflict preemption). *Id.* at 226–29.

8. *See infra* Part I.

9. For example, a plaintiff's suit against their pension plan for failure to properly disburse benefits would be preempted because ERISA provides a remedy in this situation. *See, e.g.*, Aetna Health Inc. v. Davila, 542 U.S. 200, 210 (2004) ("[I]f an individual, at some point in time, could have brought his claim under ERISA § 502(a)(1)(B), and where there is no other independent legal duty that is implicated by a defendant's actions, then the individual's cause of action is completely pre-empted by ERISA § 502(a)(1)(B).").

10. *See infra* notes 39–40 and accompanying text.

11. ADVISORY COUNCIL ON EMP. WELFARE & PENSION BENEFIT PLANS, PRIVACY AND SECURITY ISSUES AFFECTING EMPLOYEE BENEFIT PLANS 5 (2011), https://www.dol.gov/sites/dolgov/files/EBSA/about-ebsa/about-us/erisa-advisory-council/2011-privacy-and-security-issues-affecting-employee-benefit-plans.pdf [https://perma.cc/VG9W-9WSN].

12. *See id.*

laws require financial services providers to secure PII, these laws do not directly apply to benefit plans or the sensitive data that these plans hold.[13] In the absence of a comprehensive federal consumer data privacy law,[14] states have adopted their own data privacy legislation which has created a nationwide patchwork of different data privacy laws.[15]

On January 1, 2020, the California Consumer Privacy Act of 2018 ("CCPA" or the "Act")[16] went into effect, imposing strict consumer data

13. For example, the Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of 12 U.S.C. and 15 U.S.C.); The Fair Credit Reporting Act, Pub. L. No. 91-508, 84 Stat. 1114-2 (1970) (codified as amended at 15 U.S.C. § 1681); and the Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159, 117 Stat. 1952 (codified as amended at 15 U.S.C. § 1681; 20 U.S.C. § 9701-08), all address data security for financial services, but do not extend to ERISA plans. ADVISORY COUNCIL ON EMP. WELFARE & PENSION BENEFIT PLANS, CYBERSECURITY CONSIDERATIONS FOR BENEFIT PLANS 7 (2016), https://www.dol.gov/sites/dolgov/files/ebsa/about-ebsa/about-us/erisa-advisory-council/2016-cybersecurity-considerations-for-benefit-plans.pdf [https://perma.cc/VG9W-9WSN].

14. The Federal Trade Commission Act, Pub. L. No. 63-203, 38 Stat. 717 (1914) (codified as amended at 15 U.S.C. §§ 41–58), allows the Federal Trade Commission to bring enforcement actions against companies who engage in unfair or deceptive trade practices or fail to establish adequate protections of consumer data. *See* FED. TRADE COMM'N, PRIVACY AND DATA SECURITY UPDATE: 2018, at 5 (2019), https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2018/2018-privacy-data-security-report-508.pdf [https://perma.cc/CKD4-ZFGD]. However, the Federal Trade Commission Act does not mandate the comprehensive reporting and disclosure requirements that the CCPA requires and serves more as an enforcement mechanism of specific federal legislation, rather than a comprehensive data privacy law. *See generally* Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 2230, 2299 (2015) (making the case for the Federal Trade Commission to expand its enforcement role and take a more progressive stance on developing comprehensive data protection standards).

15. *See 2019 Consumer Data Privacy Legislation*, NAT'L CONF. STATE LEGISLATURES (Jan. 3, 2020), https://www.ncsl.org/research/telecommunications-and-information-technology/consumer-data-privacy.aspx [https://perma.cc/FSK3-T6VF].

16. Ch. 55, 2018 Cal. Stat. 1807 (codified as amended at CAL. CIV. CODE §§ 1798.100–.199.100 (2020)). On November 3, 2020, California passed the California Privacy Rights Act ("CPRA" or "Proposition 24") by ballot initiative. California Privacy Rights Act of 2020, Proposition 24 (Cal. 2020) (codified at CAL. CIV. CODE §§ 1798.100–.199.100 (2020)); *see* F. Paul Pittman & Kyle Levenberg, *Before the Dust Settles: The California Privacy Rights Act Ballot Initiative Modifies and Expands California Privacy Law*, WHITE & CASE TECH. NEWSFLASH (Nov. 13, 2020), https://www.whitecase.com/publications/alert/dust-settles-california-privacy-rights-act-ballot-initiative-modifies-and [https://perma.cc/62YF-A2U2]. The CPRA strengthens the CCPA by establishing the California Privacy Protection Agency, expanding consumer rights, altering the thirty-day cure period, and implementing a variety of additional data privacy and security requirements. *See* Pittman & Levenberg, *supra*. Most provisions of the CPRA become operative on January 1, 2023, with a one-year look back period for data collected in 2022. Proposition 24 § 31. The CPRA also extended the CCPA's exemption of employee data until January 1, 2023, giving employers, and consequently employer-sponsored ERISA plans, an additional year to comply. *Id.*; CAL. CIV. CODE § 1798.145(m)(1), (n)(1) (2020); *see* Anna Park, Zoe Argento & Philip Gordon, *Substantial New Privacy Obligations for California Employers: The California Privacy Rights and Enforcement Act Passes at the Polls*, LITTLER INSIGHT (Nov. 5, 2020), https://www.littler.com/publication-press/publication/substantial-new-privacy-obligations-california-employers-california [https://perma.cc/AJS7-2PEW]. Because the CCPA serves as the underlying framework for the CPRA, this Comment will refer to the CCPA when discussing the current state of California privacy law.

security and reporting requirements on covered businesses in California.[17] The Act focuses on three core consumer privacy rights: (1) the right to know about the personal information a business collects and how it uses and shares the information,[18] (2) the right to delete personal information collected by businesses (with some exceptions),[19] and (3) the right to opt out of the sale of personal information.[20] Companies that do business[21] in California and collect consumers' personal information must comply with the Act if they: (1) have annual gross revenues over $25 million; (2) annually buy, receive, or share for commercial purposes the personal information of over 50,000 consumers;[22] or

17. *See* Rachel Myrow, *California Rings in the New Year with a New Data Privacy Law*, NPR (Dec. 30, 2019, 9:00 AM), https://www.npr.org/2019/12/30/791190150/california-rings-in-the-new-year-with-a-new-data-privacy-law [https://perma.cc/5ASZ-FKRD] (describing the CCPA as "the toughest data privacy law in the U.S."); *cf.* Mary Stone Ross, *I Helped Draft California's New Privacy Law. Here's Why It Doesn't Go Far Enough*, FAST CO. (Jan. 3, 2020), https://www.fastcompany.com/90444501/i-helped-draft-californias-new-privacy-law-heres-why-it-doesnt-go-far-enough [https://perma.cc/Z4EK-5RXL] (arguing that although the CCPA is the "strictest privacy law in the country," it does not go far enough due to a weakened enforcement scheme). Although the CCPA is regarded as the strictest privacy law in the United States, it is considered less strict than the European Union's General Data Protection Regulation. Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119). Heather Kelly, *California Passes Strictest Online Privacy Law in the Country*, CNN (June 29, 2018, 12:03 PM), https://money.cnn.com/2018/06/28/technology/california-consumer-privacy-act/index.html [https://perma.cc/A6A4-4PWH].

18. *See* § 3, 2018 Cal. Stat. at 1810–11 (codified as amended at CAL. CIV. CODE § 1798.100(a)–(b) (2020)).

19. *See id.* § 3, 2018 Cal. Stat. at 1810 (codified as amended at CAL. CIV. CODE § 1798.105(a), (d) (2020)).

20. *See id.* § 3, 2018 Cal. Stat. at 1811–12 (codified as amended at CAL. CIV. CODE § 1798.120(a) (2020)).

21. The CCPA does not explicitly state what it means to "do business" in California, but the California Tax Code and judicial decisions regarding whether out-of-state companies need to register to do business in the state and whether California courts have jurisdiction over out-of-state companies likely answer this question. Matthew Stein & Christopher Lisy, *Insight: Figuring Out if You Are 'Doing Business' in California Under the CCPA*, BLOOMBERG L.: PRIV. & DATA SEC. L. NEWS (Feb. 27, 2020, 4:01 AM), https://news.bloomberglaw.com/privacy-and-data-security/insight-figuring-out-if-you-are-doing-business-in-california-under-the-ccpa [https://perma.cc/9EP2-UHN7]. The California Tax Code defines "doing business" as actively engaging in a transaction with the purpose of earning a profit, and it does not include passive investments that yield dividends. *See* Swart Enters. Inc. v. Franchise Tax Bd., 212 Cal. Rptr. 3d 670, 674 (Cal. Ct. App. 2017). If a company is not required to register with the California Secretary of State as a non-California company doing business in California, then it may not qualify as doing business in the state under the CCPA. Stein & Lisy, *supra*. Finally, companies that "purposefully avail [themselves] of the privilege of conducting activities in [California]" are likely subject to the state courts' jurisdiction and may qualify as doing business in the state. Boschetto v. Hansing, 539 F.3d 1011, 1016 (9th Cir. 2008).

22. Originally, the threshold was 50,000 consumers, § 3, 2018 Cal. Stat. at 1815 (codified as amended at CAL. CIV. CODE § 1798.140(c)(1)(B) (2020)), but the CPRA increased the threshold to 100,000, operative as of January 1, 2023, *see* California Privacy Rights Act of 2020, Proposition 24 § 14 (Cal. 2020) (codified at CAL. CIV. CODE § 1798.140(c)(1)(B) (2020)); Pittman & Levenberg, *supra* note 16.

(3) derive 50% or more of their annual revenues from selling personal information.[23] Because employee benefit plans collect personal information such as names and addresses of benefit recipients, their spouses, and their dependents, the CCPA would likely cover these plans if they operate in California and meet one of the threshold requirements.[24]

Prior to and upon its passage, speculation regarding how this landmark privacy legislation would impact employee benefit plans abounded.[25] However, analysis of the legal impact of this law on employers and businesses who store and use employee personal information, specifically employee benefit plans covered by ERISA, does not arrive at a conclusive answer. Commentators uniformly state that ERISA *may* preempt the CCPA, either completely or partially.[26] Analyzing the arguments for and against ERISA preemption of the CCPA will allow employers and plan administrators to better understand their legal obligations and predict risks associated with noncompliance. As data privacy becomes an increasingly litigated issue, courts will need to determine whether ERISA imposes a duty on employers to reasonably safeguard consumer data or whether the issue should be left to the states, which generally craft stricter privacy requirements.

Since ERISA's enactment, courts have grappled with the expansive nature of its preemption clause and its implications for state tort litigation, healthcare

23. California Consumer Privacy Act of 2018, § 3, 2018 Cal. Stat. at 1815 (codified as amended at CAL. CIV. CODE § 1798.140(c)(1) (2020)) (defining businesses covered by the CCPA).

24. *Id.*; *see* Norbert F. Kugele, *Employment Data, Employee Benefits, and the CCPA*, WARNER NORCROSS + JUDD (Jan. 16, 2020), https://www.wnj.com/Publications/Employment-Data-Employee-Benefits-and-the-CCPA [https://perma.cc/A96H-C5AK].

25. *See, e.g.*, THEODORE P. AUGUSTINOS, LAURA L. FERGUSON & EMILY HOLPERT, CCPA GUIDE: DOES PERSONAL INFORMATION INCLUDE EMPLOYEE AND EMPLOYEE BENEFIT PLAN DATA? 2 (2019), https://www.lockelord.com/-/media/privacy20190405ccpa-guide-does-personal-informatio.pdf?la=en&hash=3F74614B42724A2AA774B514F236B9A8 [https://perma.cc/A9UY-ZERG] (explaining that "ERISA-covered benefit plans that are not HIPAA-covered (such as retirement, long term disability, life and AD&D) may be able to successfully argue that personal information collected and used in connection with such plans are not subject to the requirements of the CCPA" under ERISA's preemption jurisprudence); *CCPA: Employers Should Consider Implications for Employee Benefit Plans*, HUNTON ANDREWS KURTH: PRIV. & INFO. SEC. L. BLOG (Jan. 16, 2019), https://www.huntonprivacyblog.com/2019/01/16/ccpa-employers-should-consider-implications-for-employee-benefit-plans/ [https://perma.cc/PXC2-RNCF] ("In the absence of further guidance, however, it is not certain to what extent preemption would apply – and it is also possible that a court could find that ERISA preempts some aspects of the law but not others."); Lisa Sotto, Jessica Agostinho & Danielle Dobrusin, *Where Calif. Privacy Law and Employee Benefits Data Collide*, LAW360 (Feb. 14, 2019, 3:22 PM), https://www.law360.com/articles/1127571/where-calif-privacy-law-and-employee-benefits-data-collide [https://perma.cc/4NJW-T2WA (dark archive)] ("In the absence of further guidance, however, it is not certain to what extent preemption might apply . . . .").

26. *See* Kugele, *supra* note 24. Their reluctance to come down on one side of ERISA preemption is likely because the law is unclear and untested in this area. *Id.* ("For programs subject to ERISA, there is certainly an argument that CCPA is preempted by ERISA—but California has a history of challenging ERISA preemption claims, and until courts work through that issue, it's an open question.").

administration, employment regulation, and general regulation of welfare and benefits plans.[27] But the question of whether state data privacy laws will be preempted by ERISA remains unanswered.

This Comment addresses ERISA's potential preemption of the CCPA in four parts. Part I discusses the evolution of the Supreme Court's ERISA preemption doctrine to provide context on how courts may rule on this question. Part II examines the CCPA generally and how it could impact the administration of ERISA plans. Part III presents arguments for preemption of the CCPA. Finally, Part IV argues that a likelier outcome is ERISA preempting only the parts of the CCPA that directly interfere with benefits administration.

I. THE EVOLUTION OF ERISA PREEMPTION

Over the past thirty-seven years, the Supreme Court's ERISA preemption jurisprudence has "play[ed] like an accordion with intermittent expansive interpretations and narrow interpretations."[28] This part describes (1) ERISA's two methods of preemption; (2) how the Supreme Court's interpretation of the statute has changed over time, pivoting from an expansive view of preemption to a narrower one; and (3) ERISA preemption doctrine in the context of invasion of privacy and data breach litigation.

ERISA can preempt a state law in two ways: complete preemption and express preemption. Complete preemption occurs when ERISA's text provides for civil enforcement to the absolute exclusion of other state law remedies. If a plaintiff is eligible to bring a civil action under section 502(a) of ERISA,[29] which provides a method for beneficiaries to sue to recover benefits owed under the plan or for breach of fiduciary duty,[30] then any state action is completely

27. *See, e.g.*, Cal. Div. of Lab. Standards Enf't v. Dillingham Constr., Inc., 519 U.S. 316, 334 (1997) (holding that California's prevailing wage law and apprenticeship programs were not preempted by ERISA); De Buono v. NYSA ILA Med. & Clinical Servs. Fund, 520 U.S. 806, 816 (1997) (holding that a state tax on hospitals operated by ERISA funds was not preempted under section 514(a)); Darcangelo v. Verizon Commc'ns, Inc., 292 F.3d 181, 195 (4th Cir. 2002) (holding that "state claims for invasion of privacy, negligence, unfair and deceptive trade practices, and medical privacy violations are not preempted").

28. Sharon Reece, *The Accordion Type Jurisprudence of ERISA Preemption Creates Unnecessary Uncertainty*, 88 UMKC L. REV. 115, 124 (2019).

29. If the plaintiff can prove that an independent legal duty exists outside of the duties imposed by ERISA, then section 502 may not preempt the claim. *See* Aetna Health Inc. v. Davila, 542 U.S. 200, 201 (2004).

30. Section 502(a)(1)(B) allows a beneficiary to bring a civil action to "enforce his rights under the . . . plan." Employee Retirement Income Security Act of 1974, Pub. L. No. 93-406, § 502(a)(1)(B), 88 Stat. 829, 891 (codified as amended at 29 U.S.C. § 1132(a)(1)(B)). A beneficiary may also bring a civil action under section 502(a)(1)(B) to enforce the fiduciary duties owed to him under section 404(a) of the plan. *Id.*; *see also* § 404(a), 88 Stat. at 877–78 (codified as amended at 29 U.S.C. § 1104) (detailing the fiduciary duties owed to beneficiaries under ERISA).

preempted. [31] For example, a plan participant may sue under section 502(a)(1)(B) if their employer refuses to provide benefits entitled to them under the plan.[32] If the plan participant brings the claim in state court, it will be removed to federal court through a process known as complete preemption.[33]

Under section 502(a)'s complete preemption standard, a "state-law cause of action that duplicates, supplements, or supplants ERISA's civil enforcement remedy conflicts with clear congressional intent to make that remedy exclusive, and is therefore pre-empted."[34] If a state cause of action falls under ERISA's section 502 civil enforcement scheme, it is converted to a federal cause of action and removed to federal court.[35] For example, if plan beneficiaries bring state claims against their ERISA-covered plan administrator for failure to use ordinary care in the administration of benefits, then the state claims are preempted by section 502, which allows beneficiaries to directly bring suits in federal court to recover benefits due under the plan.[36]

ERISA does not specifically provide a remedy in the event of data breach or breach of privacy, likely because data breach as it occurs today was not a concern in 1974.[37] Instead, ERISA's civil enforcement remedy deals with effective management and administration of benefits.[38] Unless an individual can successfully argue that data security is a benefit as defined by ERISA and is covered by ERISA's civil enforcement scheme, section 502 likely does not apply to consumers' data security and claims related to data breach.

31. *See Aetna Health Inc.*, 542 U.S. at 201 ("If an individual . . . could have brought his claim under ERISA § 502(a)(1)(B), . . . the individual's cause of action is completely pre-empted by ERISA § 502(a)(1)(B).").

32. § 502(a)(1)(B), 88 Stat. at 891.

33. *See Aetna Health Inc.*, 542 U.S. at 200 (citing Beneficial Nat'l. Bank v. Anderson, 539 U.S. 1, 8 (2003)).

34. *Id.* at 200–01.

35. *Id.* at 209.

36. *See id.* at 212–14 (holding that the plaintiffs' state law claims alleging lack of care when making healthcare benefits decisions were preempted by section 502(a) of ERISA). If a plaintiff brings a claim under section 502 (rather than a state law tort claim), they may only obtain denied benefits and not punitive damages even if they were denied benefits in bad faith or by a tortious act. *See* Pilot Life Ins. Co. v. Dedeaux, 481 U.S. 41, 53–54 (1987) ("Relief may take the form of accrued benefits due, a declaratory judgment on entitlement to benefits, or an injunction against a plan administrator's improper refusal to pay benefits. A participant or beneficiary may also bring a cause of action for breach of fiduciary duty, and under this cause of action may seek removal of the fiduciary.").

37. ERISA does not explicitly require fiduciaries to protect against data breach, but it does establish a general duty for the fiduciary to "discharge his duties with respect to a plan solely in the interest of the participants and beneficiaries and for the exclusive purpose of providing benefits to participants and their beneficiaries; and defraying reasonable expenses of administering the plan." Employee Retirement Income Security Act of 1974, § 404(a)(1)(A), 88 Stat. at 877 (codified as amended at 29 U.S.C. § 1104(a)(1)(A)). Fiduciaries may face personal liability for any plan losses resulting from a breach of duty. *See id.* § 409(a), 88 Stat. at 886 (codified at 29 U.S.C. § 1109(a)).

38. *See id.* § 502, 88 Stat. at 891–93 (codified as amended at 29 U.S.C. § 1132).

The second and most debated method of ERISA preemption, express preemption, is located in section 514(a). Section 514(a) of ERISA explicitly preempts all state laws "insofar as they may . . . relate to an employee benefit plan."[39] ERISA does not define the meaning of relates to but does exclude several areas of state law from preemption, including state banking, securities, and insurance laws, as well as "generally applicable criminal laws."[40] Due to the lack of explicit statutory guidance regarding the scope of what relates to employee benefit plans, express preemption has been applied inconsistently.

A. *The Supreme Court's Inconsistent Application of Section 514 Express Preemption Perpetuates Uncertainty in This Area*

ERISA section 514(a) preempts state laws that relate to an ERISA-covered employee benefit plan.[41] Although Congress intended for this preemption clause to apply broadly,[42] the Supreme Court has limited the breadth of relate to preemption, reasoning that "[i]f 'relate to' were taken to extend to the furthest stretch of its indeterminacy, then for all practical purposes pre-emption would never run its course."[43] Consequently, the Supreme Court has further defined the boundaries of relates to as when the state's law "acts immediately and exclusively upon ERISA plans . . . or where the existence of ERISA plans is essential to the law's operation."[44] A state law may also relate to ERISA plans if it has an "impermissible connection with" the plan such that the law impacts a "central matter of plan administration."[45] Therefore, the Supreme Court's ERISA preemption jurisprudence considers both the interaction between the potentially preempted state law and the ERISA plan, as well as the state law's impact on the ERISA plan.

The Supreme Court first addressed section 514(a) ERISA preemption in *Shaw v. Delta Airlines, Inc.*[46] In *Shaw*, the plaintiffs challenged ERISA preemption of New York's Human Rights Law.[47] The state law required

39. *Id.* § 514(a), 88 Stat. at 897 (codified as amended at 29 U.S.C. § 1144(a)).

40. *Id.* § 514(b), 88 Stat. at 897 (codified as amended at 29 U.S.C. § 1144(b)).

41. *Id.* § 514(a), 88 Stat. at 897 (codified as amended at 29 U.S.C. § 1144(a)).

42. *See* 120 CONG. REC. 29,942 (1974) (statement of Sen. Javits) (discussing the need for a broad preemption standard to promote "uniformity with respect to interstate plans" and to prevent "the possibility of endless litigation over the validity of State action"); *see also* Gobeille v. Liberty Mut. Ins. Co., 136 S. Ct. 936, 943 (2016) (discussing how the Court has applied ERISA preemption to "ensure that ERISA's express pre-emption clause receives the broad scope Congress intended while avoiding the clause's susceptibility to limitless application").

43. N.Y. State Conf. of Blue Cross & Blue Shield Plans v. Travelers Ins. Co., 514 U.S. 645, 655 (1995).

44. *Gobeille*, 136 S. Ct. at 943 (quoting Cal. Div. of Lab. Standards Enf't v. Dillingham Constr., Inc., 519 U.S. 316, 325 (1997)).

45. Egelhoff v. Egelhoff *ex rel.* Breiner, 532 U.S. 141, 148 (2001).

46. 463 U.S. 85 (1983).

47. *Id.* at 92.

employers to pay benefits to employees who were unable to work due to pregnancy or other nonoccupational disabilities.[48] Delta argued that because its benefits plans were covered by ERISA, ERISA preempted the state law.[49] The Court held that any state law relates to a benefit plan if it "has a connection with or reference to" a plan.[50] Under this broad interpretation of ERISA's "plain language," the Court held that the Human Rights Law and New York Benefits Law related to the ERISA plan and were consequently preempted.[51] Although this decision allowed employers to potentially avoid compliance with the state law, the Court explicitly stated that states could require employers to structure their pregnancy and disability benefits within a separate, non-ERISA structure to avoid preemption.[52]

After *Shaw*, most state laws that referenced or impacted ERISA, even tangentially, were preempted because of this connection.[53] Twelve years later, however, the Supreme Court backtracked and restricted ERISA's broad preemptive power. In *New York State Conference of Blue Cross & Blue Shield Plans v. Travelers Insurance Co.*,[54] the Court altered its ERISA preemption doctrine, rejecting "uncritical literalism" for a narrower interpretation of the statute.[55] In *Travelers*, a New York law required hospitals to collect surcharges from commercial insurers, but not from patients insured under a Blue Cross/Blue Shield plan.[56] The Court held that ERISA did not preempt the state law, reasoning that a state law that exerts an "indirect economic influence" on a plan does not necessarily trigger preemption under ERISA.[57] The New York law created cost differences between the Blue Cross/Blue Shield plans and other plans, but it did not impact the choices that plans made when administering

48. *Id.* at 88.

49. *Id.* at 92.

50. *Id.* at 96–97.

51. *Id.* at 97.

52. *Id.* at 108 ("If the State is not satisfied that the ERISA plan comports with the requirements of its disability insurance law, it may compel the employer to maintain a separate plan that does comply."). After *Shaw*, state laws such as tort laws that applied to group benefit policies and anti-subrogation statutes that applied to self-funded medical plans were found to be preempted because they referenced or had a connection with ERISA. Edward A. Zelinsky, *ERISA Preemption After* Gobeille v. Liberty Mutual*: Completing the Retrenchment of* Shaw, 34 HOFSTRA LAB. & EMP. L.J. 301, 30 4 (2017).

53. *See, e.g.*, FMC Corp. v. Holliday, 498 U.S. 52, 66 (1990) (holding that a Pennsylvania law precluding ERISA plans from exercising subrogation rights on a plan beneficiary's tort recovery was preempted under section 514); Ingersoll-Rand Co. v. McClendon, 498 U.S. 133, 140–41 (1990) (holding that section 514 clearly preempted a state common law claim that an employee was unlawfully discharged due to his employer's desire to avoid contributing to or paying benefits under the ERISA plan).

54. 514 U.S. 645 (1995).

55. *Id.* at 656.

56. *Id.* at 649.

57. *Id.*

benefits.[58] Moreover, the Court acknowledged that rate differences between plans are common without state action and concluded that "it is unlikely that ERISA meant to bar such indirect economic influences under state law."[59] The *Travelers* decision restricted section 514(a)'s preemptive power over state law, tying preemption to statutes that relate to the core functions of the ERISA plan.

Although the Court did not find preemption in *Travelers*, it cautioned that not all state laws that indirectly impact ERISA plans will escape preemption. "[I]t is possible that state law might produce such acute, albeit indirect, economic effects as to force an ERISA plan to adopt a certain scheme of coverage or effectively restrict its choice of insurers . . . ."[60] Thus, if the state law impacts the benefits provided or participants covered, then it is likely preempted. *Travelers* refined ERISA preemption doctrine by focusing on the state law's impact on benefits provided by the plan and its administration, specifically concentrating on the core objective of ERISA—ensuring uniform administration of benefit plans—rather than any external factor that may impact the plan.

In *Travelers*, the Court altered the ERISA preemption doctrine without overruling its previous decisions. While narrowing the preemptive scope of section 514(a), the *Travelers* decision also created more uncertainty in the law because it upheld the previous *Shaw* line of cases while "simultaneous[ly] repudiat[ing] . . . the expansive reading of [section] 514(a) upon which that line is based."[61]

Following the *Travelers* decision, the Court struggled to reconcile its decision with the broader interpretation of section 514(a) preemption in *Shaw*. In holding that a California minimum wage law was not preempted by an ERISA-covered apprenticeship fund, the Court reaffirmed its narrower reading of ERISA preemption.[62] Despite concurring in the result, Justice Scalia argued that the Court should address and overrule inconsistent prior interpretations of the statute to clarify the post-*Travelers* state of the law.[63] Although the Court

58. *Id.* at 646.

59. *Id.*

60. *Id.* at 647.

61. Edward A. Zelinsky, Travelers, *Reasoned Textualism, and the New Jurisprudence of ERISA Preemption*, 21 CARDOZO L. REV. 807, 834 (1999).

62. *See* Cal. Div. of Lab. Standards Enf't v. Dillingham Constr., Inc., 519 U.S. 316, 334 (1997) ("The effect of the prevailing wage statute on ERISA-covered apprenticeship programs in California is substantially similar to the effect of New York law on ERISA plans choosing whether to provide health insurance benefits in New York through the Blues, or through a commercial carrier. The prevailing wage statute alters the incentives, but does not dictate the choices, facing ERISA plans.").

63. *Id.* at 335 (Scalia, J., concurring) ("I join the Court's opinion today because it is a fair description of our prior case law, and a fair application of the more recent of that case law. Today's opinion is no more likely than our earlier ones, however, to bring clarity to this field—precisely because it does obeisance to all our prior cases, instead of acknowledging that the criteria set forth in some of them have in effect been abandoned.").

has not explicitly overruled its early ERISA preemption opinions, its most recent decision in this area confirms a commitment to a broader interpretation of section 514(a) ERISA preemption.

Most recently, the Court held that ERISA expressly preempts state statutes directly affecting benefits administration. In *Gobeille v. Liberty Mutual Insurance Co.*,[64] the Court held that a Vermont statute requiring health insurance benefit plans to disclose claims data to a state database was preempted by ERISA.[65] Liberty Mutual, the ERISA plan administrator, was concerned that reporting claims data to the state would violate its fiduciary duty and instructed its third-party administrator[66] not to comply with the Vermont law.[67] The Court found that "reporting, disclosure, and recordkeeping are central to, and an essential part of, the uniform system of plan administration contemplated by ERISA."[68] Moreover, state laws that govern this central function of ERISA plans could create "wasteful administrative costs and threaten to subject plans to wide-ranging liability."[69] Because a primary goal of ERISA is uniform plan administration, the *Gobeille* Court held that ERISA preempts state laws that prevent uniform plan administration by requiring national plans to report claims data to a specific state database.[70]

In his concurring opinion, Justice Breyer emphasized that states may request the Department of Labor ("DOL") to provide information on ERISA plans to the state, which would achieve the preempted Vermont's statute's primary goal.[71] DOL has the authority to regulate plan reporting and administration on a federal level and to clarify how state reporting requirements affect ERISA plans.[72] Unlike some state laws, DOL regulation of ERISA plans does not carry preemption risk.

64. 136 S. Ct. 936 (2016).

65. *Id.* at 947.

66. ERISA imposes liability on any fiduciary under the plan. Cassandra G. Sasso, *Liability of Fiduciaries Under ERISA*, 21 COLO. LAW. 197, 197 (1992). A person or entity is a plan fiduciary if they exercise authority or control regarding the administration or maintenance of the plan's assets. *Id.* A third-party administrator, which is "a company that provides operational services such as claims processing and employee benefits management under contract to another company," may be liable as a fiduciary under ERISA depending on the extent of its involvement in the plan administration. Julia Kagan, *Third Party Administrator (TPA)*, INVESTOPEDIA (Aug. 30, 2019), https://www.investopedia.com/terms/t/third-party-claims-administrator.asp [https://perma.cc/H7DE-27Y5].

67. *Gobeille*, 136 S. Ct. at 942.

68. *Id.* at 945.

69. *Id.*

70. *See id.* The Court held that (1) recordkeeping and reporting were central to plan administration, and (2) allowing different states to impose different requirements on federally regulated ERISA plans would hinder the goal of uniform plan administration. *Id.* at 947.

71. *Id.* at 949 (Breyer, J., concurring).

72. *See id.*; *see also* Employee Retirement Income Security Act of 1974, Pub. L. No. 93-406, § 505, 88 Stat. 829, 894 (codified at 29 U.S.C. § 1135).

B. *State Law Claims for Tortious Invasion of Privacy Have Not Been Preempted by ERISA*

Courts have held that state tortious invasion of privacy claims against ERISA plans are not preempted because the state laws apply generally and do not directly impact the administration of benefits. For example, in *Darcangelo v. Verizon Communications, Inc.*,[73] an employee sued her employer and the administrator of her disability benefits plan alleging violations of Maryland's medical confidentiality statute and unfair and deceptive trade practices statute, as well as claims of invasion of privacy, negligence, and breach of contract.[74] The plaintiff alleged that the administrator, acting as an agent of Verizon (her employer), unlawfully obtained access to her medical records in an effort to provide Verizon with a justification for firing her.[75] Reversing the district court on all but the breach of contract claim,[76] the Fourth Circuit held that ERISA did not preempt the other state law claims because the complaint "charge[d the administrator] with conduct that [was] entirely unrelated to its duties under the ERISA plan."[77] The defendants' conduct was so far outside of ERISA's core function of plan administration that it was not acting as a fiduciary at the time of the alleged misconduct.[78] Consequently, the claims were not related to a core function of ERISA because the defendants were not acting in furtherance of ERISA's central goals.[79]

Although *Darcangelo* does not specifically address invasion of privacy claims and ERISA, it generally holds that wrongful actions by employers and plan administrators that go beyond ordinary operations of the plan do not escape state law just because they are associated with ERISA. It is notable that, rather than failing to protect an employee's privacy, the defendants in *Darcangelo* allegedly acted *affirmatively* to invade the employee's privacy.[80]

Similarly, in *Dishman v. UNUM Life Insurance Co. of America*,[81] the Ninth Circuit held that tortious conduct only loosely related to plan administration is not preempted by ERISA.[82] There, the plaintiff sued the insurance company

73. 292 F.3d 181 (4th Cir. 2002).

74. *Id.* at 186.

75. *Id.*

76. The court held that the breach of contract claim was "completely preempted and [was] transformed into a federal claim under ERISA [section] 502." *Id.* at 187.

77. *Id.* at 186.

78. *Id.* at 192–93.

79. *See id.*

80. In contrast, data breach claims often allege that a defendant failed to take prudent precautions to secure data and protect a plan participant's privacy. A court may be more likely to conclude that a plan administrator who fails to secure participants' data is acting within the confines of ERISA plan administration, and consequently, a negligence claim brought by a plan fiduciary after a data breach would be preempted. *See* Moran, *supra* note 3, at 504.

81. 269 F.3d 974 (9th Cir. 2001).

82. *Id.* at 979–80.

that administered his employer's long-term disability benefits plan in an effort to challenge the suspension of his disability benefits and demonstrate that the insurer was vicariously liable for tortious invasion of privacy by its investigators.[83] UNUM initially granted Dishman's claim for disability benefits but later investigated the claim.[84] Dishman alleged that an investigator retained by UNUM wrongfully elicited personal information about him by: (1) claiming to be a bank loan officer to verify information about him, (2) falsely representing that he had volunteered to coach a basketball team, (3) impersonating him to get credit card information and travel itineraries, and (4) repeatedly calling and photographing his residence.[85] The Ninth Circuit held that, although "there [was] clearly some relationship between the conduct alleged and the administration of the plan, it is not enough of a relationship to warrant preemption."[86] Because the defendant's conduct was more of a "garden-variety" tort rather than an act of plan administration, Dishman's state common law tort action was not preempted under section 514(a).[87]

C. *State Data Breach Laws Likely Escape ERISA Preemption*

The Supreme Court has not yet addressed ERISA preemption of state data privacy and data breach laws.[88] However, two district court cases recently considered whether ERISA preempts state data privacy laws. These cases illustrate two central questions that arise when looking at the interaction between state data privacy laws and ERISA. First, is data privacy, or the reasonable attempt to keep consumer personal information private, a benefit as defined by ERISA? And second, do state data privacy laws affect the uniform administration of ERISA plans?

In a Ninth Circuit class action data breach case, *In re Anthem, Inc. Data Breach Litigation*,[89] a California district court held that the defendants' claims were neither completely nor expressly preempted by ERISA.[90] The court declined to extend the definition of plan benefit under ERISA to include data security because ERISA defines benefits as insurance-type payments or coverage for healthcare-related services, and thus found no section 502 complete

83. *Id.* at 979.

84. *Id.* at 978.

85. *Id.* at 979–80.

86. *Id.* at 984.

87. *Id.*

88. Although not related to data privacy, the Ninth Circuit did rule that a state law claim for tortious invasion of privacy was not preempted by ERISA. Dishman v. UNUM Life Ins. Co. of Am., 269 F.3d 974, 982 (9th Cir. 2001) (holding that pursuing a tortious invasion of privacy action against plan administrators would not interfere with the uniform administration of benefits because it would not require administrators to "vary their administration of benefits state by state").

89. No. 15-MD-02617, 2016 WL 3029783 (N.D. Cal. May 27, 2016).

90. *Id.* at *48, *50.

preemption.[91] When analyzing express preemption, the court determined that "laws that implicate the administration of ERISA benefits are subject to express preemption, and laws that do not are not preempted."[92] It reasoned that the state laws applicable to the plaintiffs' argument qualified as "laws of general application, and do not focus exclusively (or, for that matter, even primarily) upon ERISA plan administration."[93] Because the plaintiffs' state law claims[94] did not "implicate the administration of ERISA benefits," they were not preempted by ERISA.[95]

In *In re: Premera Blue Cross Customer Data Security Breach Litigation*,[96] an Oregon district court also held ERISA does not preempt state data security laws.[97] There, the defendant, an ERISA plan administrator, argued that the plaintiffs' claims were completely preempted because they could have been brought under ERISA's section 502 civil enforcement scheme.[98] The Oregon court held that "the fact that data security protection is not a 'benefit' under ERISA is not determinative of whether complete preemption applies"[99] because plaintiffs may sue under section 502 to "'enforce [their] rights' under the plan."[100] The plaintiffs alleged that the express terms of their plan required Premera to provide "reasonable and adequate data security measures,"[101] and, because the plan discussed data security, the court held that "at least some of the claims . . . could have been brought under [section] 502(a)."[102] Ultimately, the *Premera* 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."[103]

These district court cases suggest that ERISA does not preempt state data breach laws. The state data breach laws generally apply to all companies, not

91. *Id.* at *48. State law claims to recover ERISA plan benefits, including healthcare costs and retirement plan disbursements, are completely preempted by ERISA section 502. *See supra* notes 29–36 and accompanying text.

92. *In re Anthem*, 2016 WL 3029783, at *50.

93. *Id.* at *49.

94. The district court reviewed plaintiffs' claims against Anthem under a number of state law claims, including one under the Georgia Insurance Information and Privacy Protection Act, ch. 39, 1982 Ga. Laws 615 (1982) (codified as amended at GA. CODE ANN. §§ 33-39-1 to -23 (LEXIS through the 2020 Reg. Sess. of the Gen. Assemb.)). *In re Anthem*, 2016 WL 3029783, at *4.

95. *In re Anthem*, 2016 WL 3029783, at *50. The court also noted that invasion of privacy claims are not subject to ERISA preemption. *Id.* (citing Dishman v. UNUM Life Ins. Co. of Am., 269 F.3d 974, 984 (9th Cir. 2001)).

96. No. 15-md-2633, 2017 WL 539578, at *1 (D. Or. Feb. 9, 2017).

97. *Id.* at *22.

98. *Id.* at *18.

99. *Id.* at *20.

100. *Id.* at *19 (quoting Aetna Health Inc. v. Davila, 542 U.S. 200, 210 (2004)).

101. *Id.* at *20.

102. *Id.* The district court determined that, because the plaintiffs were suing to enforce terms under the plan, they could have brought at least some of their claims under section 502. *Id.*

103. *Id.* at *22.

just the ERISA plan administrators. Although liability for data breach would indirectly impact the plan's administration of benefits through increased costs and risk mitigation efforts, it would not likely impact whether and how plan participants receive their benefits.

D. *ERISA Plan Fiduciaries May Have a Duty To Reasonably Protect Participant Data*

ERISA states that plan sponsors and plan administrators have a fiduciary duty to plan participants and may be personally liable for any losses a plan incurs from a data breach.[104] ERISA requires fiduciaries to discharge their duties "with the care, skill, prudence, and diligence under the circumstances" that a "prudent man . . . familiar with such matters" would use.[105] Apart from reports from the ERISA Advisory Council,[106] DOL has failed to issue conclusive regulatory guidance on plan administrators' fiduciary duty as it relates to data privacy.[107]

However, recent litigation in response to 401(k) cybersecurity breaches and distribution fraud suggests that plan sponsors and administrators may have a fiduciary duty when it comes to data privacy and security.[108] A participant in Estee Lauder's 401(k) plan sued the plan sponsor and providers alleging breach of fiduciary duty by failing to safeguard the plan assets against unauthorized distributions and failing to maintain adequate cybersecurity defenses.[109] The complaint alleged that in September or October of 2016, an unknown person or persons stole $99,000 in three different unauthorized distributions from the plaintiff's retirement account.[110] The parties later settled the case.[111]

In a similar case, *Bartnett v. Abbott Laboratories*,[112] the plaintiff sued her employer (the plan sponsor) and the retirement plan administrator for breach of fiduciary duty and violation of the Illinois Consumer Fraud and Deceptive

104. Employment Retirement Income Security Act of 1974, Pub. L. No. 93-406, § 409(a), 88 Stat. 829, 886 (codified at 29 U.S.C. § 1109(a)); *see also supra* note 37. Plan fiduciaries include anyone who provides investment advice for the plan or exercises discretionary control over the plan's operation. Usually these fiduciaries include plan trustees, administrators, and members of the plan's investment committee. *Fiduciary Responsibilities*, U.S. DEP'T LAB., https://www.dol.gov/general/topic/retirement/fiduciaryresp [https://perma.cc/V8FM-99XZ].

105. § 404(a)(1)(B), 88 Stat. at 877 (codified as amended at 29 U.S.C. § 1104(a)(1)(B)).

106. *See supra* notes 11–12 and accompanying text.

107. Moran, *supra* note 3, at 486.

108. Mamorsky, *supra* note 2.

109. Rebecca Moore, *Parties in Suit About Estee Lauder 401(k) Account Data Breach Announce Settlement*, PLANSPONSOR (Mar. 5, 2020), https://www.plansponsor.com/parties-suit-estee-lauder-401k-account-data-breach-announce-settlement/ [https://perma.cc/AEF9-MD5Z].

110. Complaint (ERISA) at 4–5, Berman v. Estee Lauder Inc., No. 19-cv-06489 (N.D. Cal. filed Oct. 9, 2019).

111. Moore, *supra* note 109.

112. No. 20-CV-02127, 2020 WL 5878015 (N.D. Ill. Oct. 2, 2020).

Practices Act[113] after an unknown third party accessed her account, changed the password, and stole $245,000 from the account.[114] The court held that the plaintiff stated a claim against the plan administrator for breach of fiduciary duty under ERISA and that the state law claims for deceptive trade practices were not preempted.[115] Similarly, a Third Circuit district court held that plan administrators have a fiduciary duty to guard against fraudulent withdrawal requests from ERISA-covered retirement accounts caused by a cybersecurity breach.[116]

Given the modern state of data security and clear frequency and danger of breach,[117] it is almost certain that ERISA fiduciaries have a duty to take some data security measures. However, plans have little guidance on what is required by federal law.[118] As data security becomes a more pressing issue, plan administrators should evaluate whether their fiduciary duty to prudently invest, administer, and protect plan assets includes a duty to protect against data breach. ERISA plans often contract with a third-party administrator to administer benefits, and this fiduciary duty to guard participant data may extend to the prudent selection of service providers.[119]

If ERISA's fiduciary duty does extend to data security and a plan participant's data is breached, the plan fiduciary still may not have necessarily breached its fiduciary duty under ERISA.[120] If the fiduciary can prove that they took appropriate measures to guard against the breach, then they will likely not be found liable.[121] However, there is no official guidance regarding what types of cybersecurity controls are appropriate and necessary in the retirement plan

113. Ch. 121 1/2, 1961 Ill. Laws 1867 (1961) (codified as amended at 815 ILL. COMP. STAT. ANN. § 505/1 (Westlaw through P.A. 101-651)).

114. *Bartnett*, 2020 WL 5878015, at *2.

115. *Id.* at *8–9.

116. *See* Leventhal v. MandMarblestone Grp., LLC, No. 18-cv-2727, 2019 WL 1953247, at *7 (E.D. Pa. May 1, 2019). The court also held that the plaintiff's state law claims for breach of contract were preempted by ERISA because they related to the plan's administration. *Id.*

117. Moran, *supra* note 3, at 490–91 ("[A]t least on some level, data breaches are unavoidable. Data thieves have the time, money, and tools to attack businesses relentlessly—in fact, hackers released around 357 million new variations of malicious programs in 2016 alone. . . . Under these circumstances, it is no wonder that so many high profile targets have suffered data breaches, including federal agencies such as the State Department, the Internal Revenue Service, and even the National Security Agency." (footnotes omitted)).

118. *Id.* at 486–87.

119. *See* Caroline E. Nelson, *Participant Data and Fiduciary Liability: The Current Regulatory Environment, the Vanderbilt Lawsuit, and Best Practices for Benefit Plan Sponsors*, MCGRATH N.: BLOG (Aug. 30, 2020), http://www.mcgrathnorth.com/employee-benefits-point-of-law/participant-data-and-fiduciary-liability-the-current-regulatory-environment-the-vanderbilt-lawsuit-and-best-practices-for-benefit-plan-sponsors/ [https://perma.cc/33Y9-2X5H].

120. Maria P. Rasmussen, *ERISA and Cybersecurity*, MCGUIREWOODS (June 5, 2016), https://www.passwordprotectedlaw.com/2016/06/erisa-and-cybersecurity/ [https://perma.cc/F7PA-WERR].

121. *Id.*

context.[122] In a recent settlement between Vanderbilt University ERISA plans and their participants,[123] the plaintiffs alleged that the university breached its fiduciary duty by allowing a third party to obtain participants' private information and to profit from that access.[124] Because the case settled, the matter of whether PII qualifies as a plan asset and thus implicates the plan's fiduciary duty remains unresolved.

To date, DOL has not issued direct guidance on security and privacy requirements for participant data.[125] However, with the frequency of data breaches and likely post-CCPA increase in litigation concerning these matters,[126] DOL or the courts should provide further guidance on this issue.

II. THE CCPA AND ERISA

Over half of all states considered consumer data privacy bills in 2019,[127] and most states have legislation that addresses the security of private consumer information such as social security numbers, credit information, or other identifying information.[128] In 2018, California passed the CCPA, which is the most expansive privacy legislation in the United States to date.[129] The CCPA requires businesses to disclose how they use consumer data and clearly provide consumers with the option to opt out of the sale of their personal data.[130] The

122. Michael Abbott & Aaron K. Tantleff, *ERISA/Cybersecurity Considerations in the COVID Age*, FOLEY & LARDNER LLP: INSIGHTS (Oct. 21, 2020), https://www.foley.com/en/insights/publications/2020/10/erisa-cybersecurity-considerations-covid-age [https://perma.cc/22HF-PG5M]. Plans may choose to apply the requirements under the Health Insurance Portability and Accountability Act ("HIPAA"), Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of 18, 26, 29, and 42 U.S.C.), for cybersecurity they already use for personal health information to PII contained in retirement plan documents. Although this is not required, it would likely provide sufficient evidence that the plan took appropriate data security measures. *See* ADVISORY COUNCIL ON EMP. WELFARE & PENSION BENEFIT PLANS, *supra* note 11, at 9.

123. Cassell v. Vanderbilt Univ., 285 F. Supp. 3d 1056, 1060 (M.D. Tenn. 2019).

124. *Id.* The plaintiffs also alleged other breaches of fiduciary duty related to the plan's investment decisions and contracting with third parties. *Id.*

125. Moran, *supra* note 3, at 486.

126. David A. Zetoony & Jena M. Valdetero, *2019 Data Breach Litigation Report*, BRYAN CAVE LEIGHTON PAISNER (May 15, 2019), https://www.bclplaw.com/en-US/thought-leadership/2019-data-breach-litigation-report.html [https://perma.cc/6RAM-5CUE].

127. Rich Ehisen, *Battles Still Rage over Calif. Data, Worker Classification Laws*, LAW360 (Oct. 4, 2019), https://www.law360.com/articles/1198833/battles-still-rage-over-calif-data-worker-classification-laws [https://perma.cc/AKG7-GNDD (dark archive)].

128. *Data Security Laws: Private Sector*, NCSL (Mar. 29, 2019), https://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx [https://perma.cc/W2R7-JWSV].

129. Max N. Helveston, *Reining in Commercial Exploitation of Consumer Data*, 123 PENN ST. L. REV. 667, 689 (2019).

130. California Consumer Privacy Act of 2018, ch. 55, § 3, 2018 Cal. Stat. 1807, 1809, 1811–12 (codified as amended at CAL. CIV. CODE §§ 1798.100(b), 1798.120(a) (2020)); *see also* Stuart D. Levi, *California Privacy Law: What Companies Should Do To Prepare in 2019*, SKADDEN (Jan. 17, 2019),

Act also makes it easier for individuals to sue businesses for data breach, providing consumers with a private right of action.[131] Because general federal privacy regulation does not rise to the level of the CCPA,[132] the Act will likely become a de facto national privacy law due to California's impact on interstate commerce.[133]

The CCPA applies to companies that do business in California and have more than $25 million in gross revenue, store data on over 50,000 consumers,[134] or make more than half of their revenue from selling consumer data.[135] The Act defines a consumer as "a natural person who is a California resident"[136] and personal information as "information that identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household."[137] However, the Act excludes information covered by a number of federal statutes,[138] including the Health Insurance Portability and Accountability Act ("HIPAA"),[139] the Fair Credit Reporting Act,[140] the Gramm-Leach-Bliley Act,[141] or the Driver's Privacy Protection Act.[142] A recent amendment to the law also excludes employment information from the Act's scope until January 1,

https://www.skadden.com/insights/publications/2019/01/2019-insights/california-privacy-law [https://perma.cc/5WYG-44AW].

131. *See* § 3, 2018 Cal. Stat. at 1821 (codified as amended at CAL. CIV. CODE § 1798.150(a)(1) (2020)).

132. However, some specific federal statutes, such as HIPAA or the Fair Credit Reporting Act, contain data security provisions. *See* 45 C.F.R. §§ 160, 164 (2019) (HIPAA Privacy Rule); *id.* §§ 164.400–.414 (HIPAA Breach Notification Rule); 15 U.S.C. § 1681s-2 (Fair Credit Reporting Act Furnisher Rule).

133. Levi, *supra* note 130 ("The law effectively sets the floor for nationwide privacy protection, since organizations may not want to maintain two privacy frameworks — one for California residents and one for all other citizens.").

134. *See supra* note 22 (explaining that this threshold will increase from 50,000 to 100,000 consumers on January 1, 2023).

135. § 3, 2018 Cal. Stat. at 1815 (codified as amended at CAL. CIV. CODE § 1798.140(c) (2020)); *California Consumer Privacy Act (CCPA)*, STATE CAL. DEP'T JUST., https://oag.ca.gov/privacy/ccpa [https://perma.cc/6N7E-YZ84].

136. § 3, 2018 Cal. Stat. at 1816 (codified as amended at CAL. CIV. CODE § 1798.140(g) (2020)).

137. *Id.* § 3, 2018 Cal. Stat. at 1817 (codified as amended at CAL. CIV. CODE § 1798.140(o)(1) (2020)).

138. *Id.* § 3, 2018 Cal. Stat. at 1820–21 (codified as amended at CAL. CIV. CODE § 1798.145(c)–(f) (2020)).

139. Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of 18, 26, 29, and 42 U.S.C.).

140. Pub. L. No. 91-508, 84 Stat. 1114 (1970) (codified as amended at 15 U.S.C. § 1681).

141. Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of 12 U.S.C. and 15 U.S.C.).

142. Pub. L. No. 103-322, 108 Stat. 1796 (1994) (codified as amended at 18 U.S.C. § 2721).

2023.[143] However, after this yearlong grace period, the CCPA will apply to all employee information.[144]

The CCPA outlines four basic consumer rights related to personal data:

> (1) the right to know what personal information a business has collected about them and how it is being used; (2) the right to "opt out" of a business selling their personal information; (3) the right to have a business delete their personal information; and (4) the right to receive equal service and pricing from a business, even if they exercise their privacy rights under the Act.[145]

The CCPA imposes comprehensive reporting requirements for businesses, and this generally includes ERISA plans unless ERISA is found to preempt the law. However, the CCPA does exempt from its scope private health information that is covered by HIPAA.[146] Therefore, most employer-sponsored health plan information is not subject to the CCPA.[147] Unlike the exemption for self-funded healthcare plans, the CCPA does not exclude retirement plans covered by ERISA. These plans may be subject to the CCPA's extensive reporting requirements, which could affect how companies and plans administer retirement benefits.

The CCPA's civil enforcement mechanism operates similarly to state data breach laws.[148] Although the California Attorney General is charged with enforcing the CCPA, the Act's civil enforcement mechanism allows consumers to bring suit against businesses in the event of a data breach.[149] If the business violates its "duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information," the affected consumer

143. *See supra* note 16 and accompanying text.

144. California Privacy Rights Act of 2020, Proposition 24 § 15 (Cal. 2020) (codified at CAL. CIV. CODE § 1798.145(m)(4), (n)(3) (2020)). The CCPA also excludes "publicly available information," which means "information that is lawfully made available from federal, state, or local government records." California Consumer Privacy Act of 2018, ch. 55, § 3, 2018 Cal. Stat. 1807, 1817 (codified as amended at CAL. CIV. CODE § 1798.145(o)(2) (2020)). Despite this definition in the Act, the precise contours of what information is publicly available remains unclear. *See* Stuart L. Pardau, *The California Consumer Privacy Act: Towards a European-Style Privacy Regime in the United States*, 23 J. TECH. L. & POL'Y 68, 93 (2018).

145. Pardau, *supra* note 144, at 72; *see also* § 3, 2018 Cal. Stat. at 1809–12 (codified as amended at CAL. CIV. CODE §§ 1798.100, 1798.105, 1798.120, 1798.125 (2020)).

146. § 3, 2018 Cal. Stat. at 1820 (codified as amended at CAL. CIV. CODE § 1798.145(c)(1) (2020)).

147. Sotto et al., *supra* note 25.

148. For a general discussion of whether state data breach laws may be preempted, see *supra* notes 89–103 and accompanying text.

149. For example, the California Attorney General may pursue legal action against businesses that violate the Act's reporting requirements, but consumers may not. Consumers may only pursue claims against entities if their data security has been compromised and only after providing the business thirty-days' written notice unless the action is solely for pecuniary damages resulting from the alleged violation. § 3, 2018 Cal. Stat. at 1821–22 (codified as amended at CAL. CIV. CODE § 1798.150(a)–(b) (2020)).

may bring suit to recover damages "not less than one hundred dollars ($100) and not greater than seven hundred and fifty dollars ($750)" per consumer, "[i]njunctive or declaratory relief," or "[a]ny other relief the court deems proper."[150] The CCPA is currently the only comprehensive state data privacy law that includes a private right of action for consumers.[151] However, this private right of action is limited to instances of data breach,[152] with the California Attorney General having enforcement authority over all other violations.[153]

The CCPA could impact ERISA plans in two ways. First, the Act's reporting and notification requirements could require ERISA plan providers to overhaul data security and compliance procedures, increasing administration costs. Second, plan sponsors and fiduciaries would face increased risk of litigation due to the civil enforcement mechanism. Companies providing ERISA-covered retirement plans could face increased legal compliance costs as well as costs associated with litigation. However, because the California Attorney General has discretionary enforcement of the Act,[154] it is also possible that noncompliant plans will not be penalized.

III. ERISA MAY PREEMPT THE CCPA BECAUSE OF THE STATE LAW'S BROAD SCOPE AND POTENTIAL IMPACT ON PLAN ADMINISTRATION

This part will examine the likelihood of complete preemption under ERISA section 502 and express preemption under section 514(a). Because ERISA does not specifically reference data security within its civil enforcement scheme (section 502), a court is more likely to find that the CCPA is expressly preempted because of its possible interference with the uniform plan administration.

150. *Id.* § 3, 2018 Cal. Stat. at 1821 (codified as amended at CAL. CIV. CODE § 1798.150(a)(1) (2020)).

151. *See* Sarah Rippy, *US State Comprehensive Privacy Law Comparison*, INT'L ASS'N PRIV. PROS., https://iapp.org/resources/article/state-comparison-table/ [https://perma.cc/8HYQ-LXXQ] (last updated Feb. 14, 2021).

152. *See* § 3, 2018 Cal. Stat. at 1821. The private right of action would likely result in increased litigation against plans in the event of data breach.

153. *See id.* § 3, 2018 Cal. Stat. at 1822 (codified as amended at CAL. CIV. CODE § 1798.155 (2020)).

154. *See* John Stephens, *California Consumer Privacy Act*, AM. BAR ASS'N (Feb. 24, 2019), https://www.americanbar.org/groups/business_law/publications/committee_newsletters/bcl/2019/201902/fa_9/ [https://perma.cc/E75B-MBDA]. On January 1, 2023, the California Attorney General will no longer enforce the Act; rather, the Act will be enforced in administrative proceedings brought by the California Privacy Protection Agency. California Privacy Rights Act of 2020, Proposition 24 § 17 (Cal. 2020) (codified at CAL. CIV. CODE § 1798.155 (2020)).

A. *ERISA Likely Does Not Completely Preempt the CCPA and Other State Data Privacy Laws Because Data Privacy Is Not a Plan Benefit*

Under section 502(a) of ERISA, a "participant or beneficiary" may bring a civil action to recover plan benefits or enforce their rights under the plan.[155] If a plaintiff brings an action to "recover benefits due," "enforce his rights under the terms of the plan," or to "clarify his rights to future benefits," the plaintiff must bring the action under ERISA's civil enforcement provision in federal court.[156] State law claims that could be brought under section 502 when no independent legal duty exists are consequently preempted, and the state court must remove the action to federal court.[157] For example, a plaintiff's breach of contract action to recover pension benefits owed to them would be preempted because section 502 of ERISA provides an enforcement scheme, and no independent legal duty is implicated outside of providing the benefits.

When plaintiffs bring claims to recover actual monetary benefits owed under a plan, it is fairly evident that section 502 will supplant the state law.[158] However, the preemption and removal decision becomes less clear when a plaintiff sues to "enforce his rights under . . . the plan." Taken at its broadest, this phrase could extend beyond rights to benefits promised by the plan and thus be interpreted to include a beneficiary's right to privacy of their personal information.[159] Preemption in this case hinges on whether the statute covers only a beneficiary's right to retain benefits or if it defines rights more broadly to include the right to security of one's personal data. Although circuit courts have not yet determined whether data security qualifies as a benefit under ERISA, several district courts have addressed the issue. In *In re Anthem, Inc. Data Breach Litigation*,[160] the court determined that data security was not a benefit under the plan, so plaintiffs' claims were not completely preempted.[161] The *In re: Premera* court also held that data security was not an ERISA plan benefit, but it found that the plaintiffs' rights under the plan had been breached because the plan expressly stated the plan's duty to protect participants'

155. Employee Retirement Income Security Act of 1974, Pub. L. No. 93-406, § 502(a), 88 Stat. 829, 891 (codified as amended at 29 U.S.C. § 1132(a)).

156. *Id.* § 502(a)(1), 88 Stat. at 891 (codified as amended at 29 U.S.C. § 1132(a)(1)).

157. *See* Metro. Life Ins. Co. v. Taylor, 481 U.S. 58, 62–63 (1987) (holding that the plaintiff's claim must be brought exclusively as a federal cause of action because the claim fell under the civil enforcement provision of ERISA).

158. *See* Pilot Life Ins. Co. v. Dedeaux, 481 U.S. 41, 54–57 (1987) (holding that ERISA's civil enforcement scheme preempted the plaintiff's state cause of action for improper benefits claims processing).

159. *See In re*: Premera Blue Cross Customer Data Sec. Breach Litig., No. 15-md-2633, 2017 WL 539578, at *20 (D. Or. Feb. 9, 2017).

160. No. 15-MD-026170, 2016 WL 3029783 (N.D. Cal. May 27, 2016).

161. *Id.* at *47–48.

privacy.[162] However, the court ultimately held that the state law imposed an independent legal duty apart from the ERISA plan such that complete preemption did not apply.[163]

It is likely that a court would not find the CCPA's private right of action completely preempted by ERISA. ERISA's limited definition of benefits does not explicitly include data security and instead focuses on members' rights in relation to the administration of those benefits. Thus, unless specifically included in plan documents, plan participants likely do not have a right to data security under the plan.[164] When Congress passed ERISA, it did not address consumers' rights related to privacy and data security.[165] Congress intended to pass a scheme of comprehensive legislation to protect the benefit expectations of workers while promoting the growth of these pension plans,[166] but Congress almost certainly did not intend for ERISA to regulate data privacy as well.

Although ERISA does not address data security and privacy, it does impose a fiduciary duty on plans and their administrators.[167] ERISA requires plan fiduciaries to act "with care, skill, prudence, and diligence under the circumstances then prevailing that a prudent man acting in a like capacity and familiar with such matters would use."[168] The issue here is whether allowing a data breach to occur or inadvertently disclosing members' personal information would constitute breach of fiduciary duty such that plaintiffs could seek damages under section 502.

If a court determines that protecting against data breach falls within the ERISA fiduciary duty, then state data breach claims would be completely preempted. If plaintiffs successfully allege breach of fiduciary duty, they must also successfully argue that there was an injury-in-fact.[169] With the current

162. *In re: Premera*, 2017 WL 539578, at *20–22 (finding that, because the plan documents included data privacy provisions, at least some of the plaintiffs' claims could have been brought under section 502(a) "to enforce their alleged rights under their ERISA plan").

163. *Id.* at *22 ("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.").

164. *See supra* notes 29–38 and accompanying text.

165. Moran, *supra* note 3, at 498.

166. Cohen, *supra* note 5, at 589.

167. *See* Employee Retirement Income Security Act of 1974, Pub. L. No. 93-406, § 404, 88 Stat. 829, 877–78 (codified as amended at 29 U.S.C. § 1104); *see also supra* note 104.

168. § 404(a)(1)(B), 88 Stat. at 877 (codified as amended at 29 U.S.C. § 1104(a)(1)(B)).

169. John Utz, *Privacy Risks for Non-Health Benefit Plans*, LAW360 (July 2, 2018, 1:09 PM), https://www.law360.com/articles/1055852/privacy-risks-for-non-health-employee-benefit-plans [https://perma.cc/4643-X99P (dark archive)] ("To sue in federal court the participant must have an injury-in-fact within the meaning of Article III of the Constitution, and must also have suffered an injury to have recourse under ERISA."). The Supreme Court has held that to establish standing in federal court a plaintiff must prove that they experienced a "concrete and particularized" injury. Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1548 (2016) (quoting Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 (1992)). A "bare procedural [statutory] violation" without the risk of real harm

frequency of data breach, plaintiffs could have a difficult time proving that the fiduciary's irresponsible management or failure to act was the proximate cause of the injury and that the breach of personal information could not have just as likely been caused by a non-ERISA entity.[170]

It is possible that a court would find complete preemption of a claim for damages caused by data breach, but not likely. Courts have generally interpreted the ERISA fiduciary duty narrowly, focusing on prudent investment of pension plans and administration of benefits.[171] A court would more likely determine preemption based on ERISA's section 514 express preemption provision because the CCPA imposes an independent legal duty on plans to guard against data breach and respond to privacy threats.[172]

B. *Whether ERISA Section 514(a) Expressly Preempts the CCPA Depends on How Broadly a Court Interprets "Relates to"*

ERISA section 514(a) preempts state laws that relate to any ERISA plan.[173] A law relates to an ERISA plan (1) if it explicitly references the plan[174] or (2) if the state law has an "impermissible 'connection with'" the plan such that it "'governs . . . a central matter of plan administration' or 'interferes with

does not satisfy the concreteness requirement. *Id.* at 1550. Courts look to history and congressional intent to determine whether an injury—tangible or intangible—occurred, and the individual plaintiff must have personally suffered the injury. *Id.* at 1548–49. Plaintiffs meet the standing requirement when they actually experience identity theft resulting from a data breach; however, circuits differ on whether an alleged risk of future harm from data breach is substantial enough to meet the Article III standing requirement. *See* Attias v. Carefirst, Inc., 865 F.3d 620, 627 (D.C. Cir. 2017); *see also* Nancy R. Thomas, *No Injury, No Data Breach Claims? Depends on the Circuit*, MORRISONFOERSTER (Sept. 17, 2020), https://www.mofo.com/resources/insights/200917-no-data-breach-claims.html [https://perma.cc/9ZJX-BBWX] (discussing how the Sixth, Seventh, Ninth, and D.C. Circuits have found that the alleged risk of future harm meets Article III standing and the Third, Fourth, and Eighth have found that it does not).

170. Utz, *supra* note 169. Because data breaches are common and affect so many people, it is hard for plaintiffs to prove that the loss of their personal information was caused by a breach at a specific company. *See* Nicole Hong, *For Consumers, Injury Is Hard To Prove in Data-Breach Cases*, WALL ST. J. (June 26, 2016, 8:06 PM), https://www.wsj.com/articles/for-consumers-injury-is-hard-to-prove-in-data-breach-cases-1466985988 [https://perma.cc/A4CN-UAGA] ("Companies say having personal data compromised doesn't necessarily equate to an injury that merits compensation. Even when real harm occurs, such as when stolen credit-card information is used for fraudulent purchases, customers often struggle to prove that the fraud stemmed from a breach at one particular company. What's more, banks typically reimburse their customers for fraudulent charges.").

171. *See, e.g.*, *In re*: Premera Blue Cross Customer Data Sec. Breach Litig., No. 15-md-2633, 2017 WL 539578, at *21–22 (D. Or. Feb. 9, 2017).

172. *See* California Consumer Privacy Act of 2018, ch. 55, § 3, 2018 Cal. Stat. 1807, 1821–22 (codified as amended at CAL. CIV. CODE § 1798.150 (2020)).

173. Employment Retirement Income Security Act of 1974, § 514(a), 88 Stat. at 897 (codified as amended at 29 U.S.C. § 1144(a)).

174. District of Columbia v. Greater Wash. Bd. of Trade, 506 U.S. 125, 129–30 (1992) ("ERISA pre-empts any state law that refers to . . . covered benefit plans . . . .").

nationally uniform plan administration.'"[175] For example, the Supreme Court held that a Vermont law requiring ERISA health benefit plans to report claims data to a state database was preempted because the law's requirements were impermissibly connected to ERISA such that compliance would burden plan administration.[176]

The CCPA exempts some entities covered by federal law from compliance,[177] but it does not exempt ERISA-covered nonhealthcare plans, such as employee benefit plans. Because the CCPA does not explicitly reference ERISA, preemption hinges on whether there is an impermissible connection between the state law and ERISA that governs a central matter of plan administration or interferes with nationally uniform plan administration.

Courts must consider whether data security and privacy constitute a "central matter of plan administration."[178] Although data security measures have become ubiquitous if not mandatory, ERISA's central matters concern the regulation of welfare benefits and retirement income for plan participants.[179] Moreover, ERISA does not reference data security or privacy within its text.[180] Proponents of preemption may argue that the nature of personal information collected by plans and the extensive reporting requirements within ERISA indicate that data privacy has become a central matter of plan administration.[181] Additionally, a court could find that the reporting and recordkeeping requirements imposed by the CCPA are a central part of plan administration and thus expressly preempted by ERISA.[182] Overall, preemption hinges on whether the CCPA imposes "direct regulation of a fundamental ERISA function" that would impact the uniform administration of the plan.[183] ERISA plans will likely argue that collecting and maintaining participant data is an essential part of plan administration because it directly impacts the plan's ability to provide benefits to its participants. When a pension plan must follow a different set of regulations for its California participants, there is an argument

175. Gobeille v. Liberty Mut. Ins. Co., 136 S. Ct. 936, 943 (2016) (quoting Egelhoff v. Egelhoff *ex rel.* Breiner, 532 U.S. 141, 148 (2001)).

176. *See supra* notes 64–70 and accompanying text.

177. *See* California Consumer Privacy Act of 2018, § 3, 2018 Cal. Stat. at 1820–21 (codified as amended at CAL. CIV. CODE § 1798.145 (2020)).

178. *Gobeille*, 136 S. Ct. at 943 (quoting Egelhoff v. Egelhoff *ex rel.* Breiner, 532 U.S. 141, 148 (2001)).

179. *See* Cohen, *supra* note 5, at 589.

180. *See* Moran, *supra* note 3, at 498.

181. In fact, some ERISA-covered retirement plans share consumer data to promote other financial products. *See* John Manganaro, *Vanderbilt Settlement Agreement Prohibits Data-Based Cross Selling*, PLANADVISER (Apr. 29, 2019), https://www.planadviser.com/vanderbilt-settlement-agreement-prohibits-data-based-cross-selling/ [https://perma.cc/5FGD-DJMD].

182. Most recently, the Supreme Court held that a Vermont state law requiring healthcare plans to submit claims records to a state database "enter[ed] a fundamental area of ERISA regulation" and was thus preempted. *Gobeille*, 136 S. Ct. at 946.

183. *Id.*

that the regulations directly impact the uniform administration of benefits and thus the CCPA relates to ERISA.

If ERISA does preempt the CCPA, the lack of regulation of ERISA-member PII will likely persist unless ERISA is amended to include specific data privacy regulations or Congress enacts a national privacy law. Without further guidance from DOL or the courts, plans may choose to comply with the CCPA rather than risk the consequences of noncompliance.

IV. THE CASE AGAINST PREEMPTION

When evaluating the ERISA preemption question, the Supreme Court has instructed that courts begin with a presumption against preemption because ERISA was not intended to replace all state laws.[184] Following the Court's analysis in *Gobeille*, preemption hinges on two questions. First, does the state law act immediately or exclusively upon the ERISA plan?[185] Second, does the act govern a central matter of plan administration or interfere with a nationally uniform system of administration?[186] At the same time, the Court has held that ERISA does not preempt state laws of general applicability.[187] Thus, if a court finds that ERISA does not preempt the CCPA, it will likely focus on the general applicability of the CCPA and on ERISA's silence regarding data security.[188]

This part discusses reasons why the CCPA may escape preemption and determines that partial preemption of the CCPA's reporting and disclosure requirements is the most likely outcome.

A. *Obligations Imposed by the CCPA May Extend Beyond ERISA's Fiduciary Duty*

Plaintiffs seeking to avoid preemption must first overcome the section 502 complete preemption hurdle before arguing against express preemption under section 514(a).[189] Under section 502, a plan participant may bring suit to recover *benefits* promised under the plan.[190] The district court in *In re Anthem* concluded that section 502 civil enforcement rights only pertain to a plaintiff's rights to

184. De Buono v. NYSA-ILA Med. & Clinical Servs. Fund, 520 U.S. 806, 814 (1997).

185. *Gobeille*, 136 S. Ct. at 943.

186. *Id.*

187. *See, e.g.*, *De Buono*, 520 U.S. at 814–15; Cal. Div. of Lab. Standards Enf't v. Dillingham Constr., Inc., 519 U.S. 316, 334 (1997).

188. *See In re*: Premera Blue Cross Customer Data Sec. Breach Litig., No. 3:15-MD-2633, 2017 WL 539578, at *20–22 (D. Or. Feb. 9, 2017); *In re* Anthem, Inc. Data Breach Litig., No. 15-MD-02617, 2016 WL 3029783, at *49 (N.D. Cal. May 27, 2016).

189. *See supra* notes 29–40 and accompanying text.

190. Employee Retirement Income Security Act of 1974, Pub. L. No. 93-406, § 502(a)(1)(B), 88 Stat. 829, 891 (codified as amended at 29 U.S.C. § 1132(a)(1)(B)).

retain benefits under the plan.[191] The court then discussed whether protecting customer PII qualifies as an ERISA benefit.[192] Although ERISA does not define "benefit," subsections consistently refer to benefits as payments for healthcare-related services or payments sent to beneficiaries.[193] As such, courts have generally construed benefits narrowly.[194] Even a medical reimbursement claim was not considered a benefit under section 502 complete preemption when the claim related to the ERISA plan or when section 502 could provide a similar remedy.[195] Ultimately, the court stressed "the importance of construing ERISA benefits in a narrow manner," and because ERISA is silent on privacy obligations, the court declined to extend complete preemption.[196]

In *In re: Premera*, the district court extended complete preemption despite acknowledging that data privacy is not a benefit as defined by ERISA.[197] Because Congress did not include the term benefit in the second type of section 502 claims (to enforce rights under the plan) but did include benefit in the first and third claim types,[198] the court reasoned that Congress intended for rights to extend beyond plan benefits.[199] Thus, the complete preemption question partially hinged on whether the plan included "data security promises."[200] If the plan did include data security promises and the plan failed to uphold those promises, then claims to enforce those rights under the plan could have been brought under section 502.[201]

Although the *In re: Premera* court found some of the plaintiffs' claims completely preempted, the plan's independent legal duty to "reasonably and adequately" protect participants' data prevented complete preemption over all claims.[202] Because the plan sponsor had a duty to protect participants' PII under

191. *In re Anthem*, 2016 WL 3029783, at *47. ("To put it another way, ERISA complete preemption applies where ERISA benefits are at issue, and does not apply when ERISA benefits are not at issue.").

192. *See id.*

193. *Id.*

194. *See, e.g.*, *id.* at *47–48 (discussing the Ninth Circuit's holding in Marin Gen. Hosp. v. Modesto & Empire Traction Co., 581 F.3d 941 (9th Cir. 2009)).

195. *See id.*

196. *Id.* at *48.

197. *In re*: Premera Blue Cross Customer Data Sec. Breach Litig., No. 15-md-2633, 2017 WL 539578, at *20 (D. Or. Feb. 9, 2017).

198. *See id.* at *18 (discussing a beneficiary's ability "to enforce his or her rights under the plan" without reference to a benefit in the second type of claim available under section 502).

199. *See id.* at *18–19 ("The Court's interpretation that the second type of claim does not solely involve rights to 'benefits' is also supported by the Supreme Court's description of the types of claims under section 502(a)(1)(B). The Supreme Court noted that '[i]f a participant or beneficiary believes that benefits promised to him under the terms of the plan are not provided, he can bring suit seeking provision of those benefits. A participant or beneficiary can *also* bring suit generically to "enforce his rights" under the plan, or to clarify any of his rights to future benefits.'" (quoting Aetna Health Inc. v. Davila, 542 U.S. 200, 210 (2004))).

200. *Id.* at *20.

201. *Id.*

202. *Id.* at *20–22.

state law, HIPAA, and industry standards, the plaintiffs' claims were not solely based on the plan's fiduciary duty under ERISA.[203]

B. *The CCPA's General Applicability May Save It from Preemption*

The strongest argument against express preemption of the CCPA is the Act's general applicability to businesses throughout California. It "function[s] irrespective of the existence of an ERISA plan" and consequently should not be preempted.[204] Opponents of preemption may argue that the goals of the CCPA fall within the traditional state police power to regulate businesses in the interest of consumers and thus should not be preempted.

Generally applicable state laws may impact ERISA plans, but that does not necessarily mean that ERISA preempts them. When evaluating whether ERISA preempted a California state tax law,[205] the Second Circuit further discussed the types of generally applicable laws that have not been preempted including:

> (1) a generally applicable garnishment law under which creditors may garnish ERISA welfare benefits; (2) a law requiring companies to make lump-sum severance payments when closing a plant; (3) a law prescribing the amount that hospitals can charge for care; and (4) a city *income tax* of general application that affects employee contributions to benefit plans.[206]

The Court of Appeals for the Second Circuit thus distinguished between state laws that may impact ERISA plans and laws that control ERISA plan decisions—with only the latter triggering preemption.[207]

The Supreme Court addressed state regulation of healthcare in *Travelers*, noting that reading all state laws that impact the costs of healthcare plans as preempted would displace state law and contradict the intent of the statute.[208] The consumer privacy regulation within the CCPA, like healthcare regulation, may impact the cost of retirement plans, but it also generally applies to all

203. *Id.* at *21.

204. *Id.* at *22 (arguing that the state law is not preempted because the existence of an ERISA plan is not essential for the state law to operate).

205. Hattem v. Schwarzenegger, 449 F.3d 423, 431 (2d Cir. 2006) (holding that California's unrelated business taxable income exemption system was not preempted by ERISA because "taxation is a realm of historic state control" and does not have an impermissible "connection with" an ERISA plan even though the law "may have an indirect effect on [investment] choices").

206. *Id.* at 430–31.

207. *Id.* at 431.

208. *See* N.Y. State Conf. of Blue Cross & Blue Shield Plans v. Travelers Ins. Co., 514 U.S. 645, 661 (1995) ("Indeed, to read the pre-emption provision as displacing all state laws affecting costs and charges on the theory that they indirectly relate to ERISA plans that purchase insurance policies or HMO memberships that would cover such services would effectively read the limiting language in § 514(a) out of the statute, a conclusion that would violate basic principles of statutory interpretation . . . .").

California residents and large businesses transacting in California.[209] Allowing preemption in this case would invalidate a state law regulating an area in which federal legislation remains silent. Moreover, allowing ERISA plans to sidestep state data privacy laws could put participants' benefits at risk, which is contrary to the statute's intent.[210]

C. *A Likely Outcome: Partial Preemption*

If faced with the ERISA preemption question regarding the CCPA, courts may look to the functional aspects of the state law to determine whether a part of the Act relates to an ERISA plan. A court will likely rule that aspects of the CCPA directly affecting the ERISA plan's reporting, disclosure, and benefits-administration functions are preempted, but general CCPA provisions dealing with consumer rights and privacy are not preempted. For example, the CCPA grants consumers the right to request specific information that businesses collect about them.[211] This consumer right is not afforded to ERISA plan participants specifically, so it likely would not be preempted because it generally applies to all consumers and does not relate to a central function of an ERISA plan. Nonetheless, ERISA may preempt the CCPA's requirement that businesses disclose the type of information they collect to consumers because it conflicts with a central reporting function associated with the administration of the plan.[212]

The CCPA's private right of action for data breach will likely not be preempted if a court finds that guarding against data breach constitutes an "independent legal duty"[213] apart from ERISA's fiduciary duty. Recent Ninth Circuit litigation[214] supports existence of an independent legal duty. But it is important to note that allowing consumers to sue ERISA plans or their fiduciaries in response to data breach does not necessarily mean that plans will ultimately be held responsible. If plan fiduciaries establish that they were not negligent because they implemented reasonable procedures to guard against the data breach, then they will not be held responsible. The possibility that ERISA does not preempt the CCPA may spur plan sponsors and administrators to

209. *See* Sara H. Jodka, *California's Data Privacy Law: What It Is and How To Comply (A Step-by-Step Guide)*, DICKINSON WRIGHT (July 2018), https://www.dickinson-wright.com/news-alerts/californias-data-privacy-law [https://perma.cc/82KD-LEH8].

210. *See supra* note 5 and accompanying text.

211. California Consumer Privacy Act of 2018, ch. 55, § 3, 2018 Cal. Stat. 1807, 1810–11 (codified as amended at CAL. CIV. CODE § 1798.110(a) (2020)); Jodka, *supra* note 209.

212. *See* Gobeille v. Liberty Mut. Ins. Co., 136 S. Ct. 936, 945 (2016) ("[R]eporting, disclosure, and recordkeeping are central to, and an essential part of, the uniform system of plan administration contemplated by ERISA."). Note that *Gobeille* refers to disclosure to the state rather than disclosure to individuals. *Id.* at 939. This may impact the preemption analysis here.

213. Aetna Health Inc. v. Davila, 542 U.S. 200, 210 (2004).

214. *See supra* notes 81–87 and accompanying text.

strengthen their cybersecurity protocols, which would guard them against tort liability and better protect consumers.

Allowing the private right of action to escape preemption may increase litigation against ERISA plan sponsors and administrators, but it will also prompt ERISA plans to improve their data security protocols. Plaintiffs bringing data breach claims face an uphill battle when trying to prove their claims.[215] "[C]ircuits are split over whether individuals suffer a sufficiently concrete injury and therefore have standing to sue a business that suffered a breach when the individual's sole injury is mere loss of data resulting from the breach."[216] If a plaintiff does meet the standing requirement, they must then prove that the business negligently handled the data and that the business's negligence caused the breach.[217] The CCPA's statutory private right of action will likely result in an increase in costly litigation regardless of whether the plaintiff prevails. However, litigation risk may incentivize plan sponsors and administrators to improve their cybersecurity protocols. Absent amendments to ERISA or additional federal regulation, applying the CCPA's private right of action to ERISA plans is one of the only ways to hold plans accountable for maintaining adequate data security.

CONCLUSION

The impact of consumer privacy laws on ERISA plans remains uncertain within the legal landscape of ERISA preemption jurisprudence. ERISA's silence regarding plans' and plan administrators' responsibilities within this realm leaves the area ripe for judicial interpretation. Because ERISA does not create an explicit duty for plans to reasonably safeguard data, and the CCPA applies generally, courts should allow for provisions of the law that are not directly connected to employee benefits administration to escape preemption. This will undoubtedly impose additional administrative burdens on plans, but allowing ERISA plans to avoid such regulation provides them with an unfair "free pass" from regulation that is not benefits focused. If California intended for ERISA plans to avoid CCPA compliance, it would have included them in the legislative carve out. When deciding if ERISA preempts the CCPA, courts should adhere to the traditional "presumption against preemption" and preempt only aspects of the CCPA that relate to its core objective of uniform administration of plan benefits.

215. *See* Moran, *supra* note 3, at 494.

216. *Id.*

217. *See id.* at 494–95. Proving causation becomes increasingly difficult because of the ubiquity of data theft and breach caused by unknown sources. *Id.*

KATHERINE Q. MORROW**

** I would like to thank Laura Nolen, Professor Jolynn Dellinger, Professor Anne Klinefelter, and Jessica O'Brien for their guidance in developing this Comment. I would also like to thank my Primary Editor, Morgan Maccherone, and the Board and Staff Members of the *North Carolina Law Review* for their thoughtful edits and hard work throughout the publishing process.