EPSTEIN
BECKER
GREEN

ERISA Fiduciary Duty and Liability and Data Security of Employee Benefit Plans

Cybersecurity Risks for Employee Benefit Plans

New York City Bar Association, November 14, 2019

Michelle Capezza

Presented by

Michelle Capezza
Member of the Firm
mcapezza@ebglaw.com
212-351-4774

EPSTEIN BECKER GREEN

Segment I-Understanding Fiduciary Responsibilities and Potential Claims

- Who are the ERISA plan fiduciaries?
- What are the fiduciary responsibilities under ERISA?
- Who can bring fiduciary breach claims under ERISA?
- Are there potential fiduciary breach claims related to participant data privacy and security in benefit plans?
- What is the current landscape of laws that affect data privacy and security?

ERISA Plan Fiduciaries

- Fiduciaries include individuals or entities who:
  - Exercise any discretionary authority or control over the management of the plan or management or disposition of plan assets
  - Render investment advice to the plan for a fee
  - Have discretionary authority or responsibility in plan administration
  - Fiduciaries are “named” in the plan documents and other individuals can be fiduciaries based on their functions
- Fiduciaries include:
  - Plan Sponsor
  - Plan Administrator
  - Plan Benefits Committee Members
  - Plan Trustee
  - Plan Investment Advisers
  - Individuals exercising discretion in the administration of the Plan

ERISA Plan Fiduciary Responsibilities

- Fiduciary responsibilities include:
  - Acting solely in the interest of plan participants and beneficiaries with the exclusive purpose of providing benefits to them (duty of undivided loyalty)
    - E.g., ensure timely remittance of employee contributions, maintain plan records, claims procedures, avoid misleading statements and misrepresentations
  - Use plan assets for the exclusive purpose of paying plan benefits or defraying reasonable expenses of administering the plan (exclusive benefit rule)
  - Carrying out duties with care, skill, prudence and diligence (prudent person rule)(e.g., develop prudent processes and procedures to demonstrate prudent decision making which can include Investment Policy Statement, Retirement Committee meetings and Minutes, RFPs for service providers)
  - Diversifying plan investments to minimize risk of large losses (diversification rule)
  - Following plan document terms (unless inconsistent with ERISA), interpreting provisions, maintaining plan documents

ERISA Plan Fiduciary Responsibilities

Examples continued:

- Meeting applicable reporting and disclosure requirements (*e.g.*, Form 5500 filings, SPDs, SMMs, SARs, benefit statements, fee disclosures, QDIA notice, safe harbor notice, 204(h) notice, blackout notice, plan documents upon request)
- Prudently selecting and monitoring all those to whom responsibilities have been delegated, the performance of service providers, plan services, investment options and reasonableness of fees
- Timely depositing plan contributions
- Meeting the bonding requirement
- Avoiding prohibited transactions (e.g., certain transactions with parties in interest, self dealing, acting adversely to participants or beneficiaries)

Who Can Bring Fiduciary Breach Claims Under ERISA

- A civil action under ERISA Section 502(a)(2) can be brought against a fiduciary for breach of its fiduciary duties by:
  - Participants
  - Beneficiaries
  - Co-Fiduciaries
  - The Secretary of Labor

  For appropriate relief under ERISA Section 409:
  - Personal liability for loss caused to the plan
  - Personal liability to restore to the plan any profits that the fiduciary made to through the use of plan assets
  - Other equitable or remedial relief a court deems appropriate, including removal of the fiduciary

What Must a Plaintiff Prove in an ERISA Section 502(a)(2) Claim?

- For this claim of breach of fiduciary duty, the plaintiff must:
  - Prove a plan fiduciary breached its ERISA fiduciary duty
  - Show that there was a loss to the plan because of the breach

  See, e.g., Leckey v. Stefano, 501 F.3d 212, 225-26 (3d Cir. 2007).

  Circuit courts are split on who must prove causation-some Circuits have held that the fiduciary must prove that a loss was not caused by the breach of duty.

  Relief can be provided to the plan as a whole, not to award relief to individuals in compensatory or punitive damages. *See Massachusetts Mutual Life Insurance Co. v. Russell*, 473 U.S. 134 (1985).

  However, the U.S. Supreme Court later found that this does authorize recovery for fiduciary breaches that impair the value of plan assets in a participant's individual account under a defined contribution plan because each account is in essence a plan that can suffer loss. *See LaRue v. DeWolff, Boberg & Associates, Inc., et. al., 552 U.S. 248 (2008).*

Other Potential ERISA Claims

- ERISA Section 502(a)(3)
  - Participants and beneficiaries can sue for individual relief to remedy fiduciary breaches and not for relief for the plan under ERISA Sections 502(a)(3) where the remedy for a successful claim is equitable relief for individual harm (the DOL can sue for similar relief under ERISA Section 502(a)(5))
    - This section is generally viewed as the catchall provision, and normally provides relief for injuries not adequately remedied elsewhere under Section 502. *See Varity Corp. v. Howe*, 516 U.S. 489, 512 (1996).
    - To bring a claim under this section, a plaintiff must generally prove both (1) that there is a remediable wrong, *i.e.*, that the plaintiff seeks relief to redress a violation of ERISA or the terms of the Plan, *and* (2) the relief sought is appropriate equitable relief. *See*, *e.g.*, *Gabriel v. Alaska Elec. Pension Fund*, 773 F.3d 945, 954 (9th Cir. 2014).
  - A fiduciary may bring suit under ERISA Section 502(a)(3) to enjoin an act or practice which violates ERISA or the plan, or to obtain other equitable relief
  - Appropriate equitable relief:
    - "[C]ategories of relief that were typically available in equity (such as injunction, mandamus, and restitution, but not compensatory damages)." *Mertens v. Hewitt Associates*, 508 U.S. 248, 256 (1993).

Other Potential ERISA Claims

- Individual benefit claims are brought under ERISA Section 502(a)(1)(B) which allows participants and beneficiaries to bring a cause of action to challenge benefits claim denials or a declaration of benefits entitled to in the future

- These claims require a plaintiff to show that:
  - (1) plaintiff properly made a claim for benefits
  - (2) the plaintiff exhausted the plan's administrative appeals process *(if raised as a defense)*
  - (3) the plaintiff is entitled to a particular benefit under the plan's terms; *and*,
  - (4) the plaintiff was denied that benefit.

Other Avenues to Bring Claims?

- ERISA Preemption Analysis
- State Law Claims (to the extent not preempted by ERISA)
  - Breach of contract
  - Unjust enrichment
  - Promissory/Equitable Estoppel
  - Violation of state confidentiality requirements
  - Violation of state privacy laws
  - Negligence
  - Breach of covenant of good faith and fair dealing
  - Unfair or deceptive business practices

To date, no Circuit Court has applied ERISA preemption to preclude a plaintiff from moving forward with state law claims arising out of a data breach. In re Anthem, Inc. Data Breach Litigation (Settled in August 2018).

Sample of the Patchwork of Privacy and Security Laws and Regulations

There is a gap in the law for benefit plan participant and beneficiary information and data

- **Gramm-Leach-Bliley Act of 1999 ("GLBA"), 15 U.S.C. § § 6801 *et seq.***
  - Requires financial institutions that offer consumers financial products and services to respect customer privacy and protect the security and confidentiality of customers' nonpublic personal information.
- **General Data Protection Regulation (EU) 2016/679 ("GDPR")**
  - Rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.
  - Provides individual "data subjects", among other things, with the right to be forgotten or have the "controller" erase their personal data
- **SEC's Regulation S-P, 17 C.F.R. § § 248, *et seq. (see § 248.30)***
  - Requires registered broker-dealers, investment companies, and investment advisers to adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information
- **Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and The Health Information Technology for Economic and Clinical Health Act (HITECH Act) of 2009**
  - Privacy standards for the use and disclosure of protected health information; security standards to protect the confidentiality, integrity and availability of electronic PHI.
  - Expanding obligations of business associates, and additional requirements for covered entities regarding breach notifications of unsecured PHI.
- **Federal Trade Commission Act of 1914 ("FTCA")**
  - The FTCA prohibits unfair and deceptive trade practices. The FTC has brought legal actions against organizations that have violated consumers' privacy rights, or misled them by failing to maintain security for sensitive consumer information, or caused substantial consumer injury often charging the defendants with violating Section 5 of the FTC Act, which bars unfair and deceptive acts and practices in or affecting commerce. FTC also enforces other federal laws relating to consumers' privacy and security.
- **Examples of State Privacy Statutes**
  - New York's Stop Hacks and Improve Electronic Data Security Act ("SHIELD" Act) of 2019; California Consumer Privacy Act (CCPA) of 2018