THOMSON REUTERS
PRACTICAL LAW™

Cybersecurity and ERISA Fiduciary Responsibilities for Retirement Plans

by Michelle Capezza, Mintz, with Practical Law Employee Benefits & Executive Compensation

Status: **Maintained** | Jurisdiction: **United States**

This document is published by Practical Law and can be found at: **us.practicallaw.tr.com/w-024-1935**
Request a free trial and demonstration at: **us.practicallaw.tr.com/about/freetrial**

A Practice Note providing an overview of how cybersecurity may be part of the responsibilities imposed by the Employee Retirement Income Security Act of 1974 (ERISA) on fiduciaries of retirement plans.

ERISA imposes specific duties and obligations on employers, individuals involved with retirement plans, and other entities, including special rules applicable to those falling within the definition of a fiduciary in ERISA Section 3(21) (29 U.S.C. § 1002(21)).

Data and personally identifiable information (PII) have become increasingly more vulnerable to attack as they travel on employer and third-party systems. This has been partially due to the advancements in plan administration, technology, online enrollment and electronic access to account information, electronic delivery of disclosures including benefit statements, and benefit plan transaction processing (including self-certifications of distributions). In today's world, most transactions involving retirement plans are conducted electronically, including maintaining and sharing data and information across multiple platforms.

Recent cybersecurity breaches and fraudulent distributions involving retirement plans have raised the question of whether cybersecurity of plan participant information and data is a fiduciary duty under ERISA.

Fiduciaries of employee benefit plans, which are governed by ERISA, are held to a high standard of care to ensure that the plan is operated and maintained in the best interest of plan participants and beneficiaries. The extent to which ERISA fiduciary responsibility applied to the protection of plan participant and beneficiary data and PII is not statutorily explicit under current law. While there are protocols and guidance for the privacy and security of protected health information (PHI), there had not been clear protocols for ERISA plan fiduciaries to consider and follow regarding the security of PII for retirement or other benefit plans, despite their equal vulnerability to data breaches.

However, on April 14, 2021, the Department of Labor's Employee Benefits Security Administration (EBSA) issued its first formal cybersecurity best practices guidance (EBSA Cybersecurity Guidance) for:

- Plan sponsors.
- Fiduciaries.
- Recordkeepers.
- Service providers.
- Participants and beneficiaries.

The EBSA Cybersecurity Guidance:

- Is intended to help plan sponsors and fiduciaries prudently select a service provider with strong cybersecurity practices and monitor them.
- Assists plan fiduciaries and recordkeepers in their responsibilities to manage cybersecurity risks.
- Offers plan participants and beneficiaries who check their retirement accounts online basic rules to reduce the risk of fraud and loss.

The EBSA Cybersecurity Guidance is in the form of tips with suggested best practices to consider, and it is the first formal pronouncement from EBSA that ERISA plan fiduciaries are at least obligated to ensure proper mitigation of cybersecurity risk (see Legal Update, DOL Issues Cybersecurity Guidance for ERISA Retirement Plans). With the ongoing advancements in technology (including technological tools that have emerged to aid in the administration and delivery of employee benefits) and the novel cybersecurity risks that those advancements bring, there is widespread concern for the security of both:

- The employee data that is collected, transmitted, processed, and stored for employee benefit plans.
- The assets in participant accounts.

The EBSA Cybersecurity Guidance serves to complement EBSA's regulations on electronic records and disclosures to plan participants and beneficiaries (including provisions on ensuring that electronic recordkeeping systems have reasonable controls, that adequate records management practices are in place, and that electronic disclosure systems include measures calculated to protect PII).

This Note outlines the basic framework plan fiduciaries must consider for their responsibility to protect PII and data and mitigate cybersecurity risks. For guidance for plan fiduciaries to develop prudent policies and procedures to secure that information and data, see Practice Note, Best Practices for ERISA Fiduciary Responsibilities and Cybersecurity for Retirement Plans.

This Note explains:

- ERISA plan fiduciary responsibilities and cybersecurity.
- Plan assets and cybersecurity.
- Potential fiduciary liability under ERISA for retirement plan cybersecurity breaches.

ERISA Plan Fiduciaries

An ERISA fiduciary is broadly defined as any person who, regarding an employee benefit plan subject to ERISA's fiduciary duty provisions:

- Exercises any discretionary authority or control over the management of an employee benefit plan.
- Exercises any authority or control (discretionary or otherwise) over the management or disposition of plan assets.
- Provides investment advice regarding plan assets for a fee or other compensation, whether direct or indirect, or has any authority or responsibility to do so.
- Has any discretionary authority or responsibility in the administration of the plan.

(ERISA § 3(21) (29 U.S.C. § 1002(21)) and see Practice Note, ERISA Fiduciary Duties: Overview: Fiduciary Status.)

Plan fiduciaries include:

- Plan sponsors.
- Plan administrators.
- Plan benefits committee members.
- Plan trustees.
- Plan investment advisers.
- Individuals exercising discretion in the administration of the plan.

Each of these fiduciaries can have significant responsibility for cybersecurity of benefit plan data, which may include:

- Handling plan data.
- Selecting and monitoring third-party service providers.
- Developing and implementing internal cybersecurity policies and procedures.
- Addressing a cybersecurity breach.

ERISA Fiduciary Responsibilities and Cybersecurity

Neither ERISA nor federal law addresses cybersecurity and retirement plan data. However, the EBSA Cybersecurity Guidance provides tips to assist fiduciaries in meeting their responsibilities under ERISA to prudently select and monitor service providers that have strong cybersecurity practices.

If a cybersecurity breach occurs, the plan sponsor or other plan fiduciaries may be liable for a breach of fiduciary duties under ERISA, including the duties of:

- Loyalty (see Duty of Loyalty and the Exclusive Benefit Rule).
- Prudence (see Duty of Prudence).
- Acting according to plan documents (see Duty to Follow Plan Documents).

Duty of Loyalty and the Exclusive Benefit Rule

A fiduciary must act solely in the interest of plan participants and beneficiaries with the exclusive purpose of providing benefits to them. Fiduciaries must use plan assets for the exclusive purpose of providing plan benefits and defraying reasonable expenses of plan administration (the exclusive benefit rule). For example, plan fiduciaries must:

- Ensure timely remittance of employee contributions.
- Maintain plan records and claims procedures.
- Avoid misleading statements and misrepresentations.
- Review the reasonableness of plan fees and expenses.
- Make reasonable arrangements with service providers.

If plan participant data or account assets are hacked, stolen, or misused, or if the protection of participant data or actual cyberattacks are ignored, there may be grounds for asserting a breach of the duty of loyalty or exclusive benefit rule.

Plan sponsors should maintain and adhere to cybersecurity policies and procedures that demonstrate best practices to protect plan participant and beneficiary data and include a data breach response plan of action if a data breach occurs.

Included in these policies and procedures should be:

- The assembly of a qualified cybersecurity team, including individuals from HR, IT, legal, and compliance.
- The development of training programs for employees to safeguard data.
- Routine analyses and identification of the type of data collected and the interaction of that data.
- Procedures for prudent selection and monitoring of service providers with strong cybersecurity practices and negotiating service agreements.
- The utilization of cybersecurity insurance and other security technology.
- A data breach response plan.

Duty of Prudence

A fiduciary must act with the same care, skill, prudence, and diligence under the circumstances that a prudent fiduciary acting in a similar capacity and familiar with these matters is likely to use in a similar plan with the same goals. Plan fiduciaries typically develop prudent processes and procedures to demonstrate prudent decision-making in plan management, including:

- The creation of investment policy statements.
- Conducting periodic retirement committee meetings and maintaining meeting minutes.
- Conducting periodic requests for proposals (RFPs) for service providers.

In the same manner that other service providers are monitored, the plan sponsor must continue to monitor the service provider's performance as it relates to cybersecurity. Plan sponsors and fiduciaries' policies and procedures should include:

- Guidelines for engaging and monitoring service providers.
- Guidelines for renewing service provider agreements and their terms.
- Provisions for the confirmation of the cybersecurity program and certifications.
- The details regarding how data is encrypted and protected.
- Breach notification procedures.
- Procedures for safety testing (for example, penetration testing).

Duty to Follow Plan Documents

A fiduciary must act under applicable plan documents (unless inconsistent with ERISA), including plan policies and procedures. Every plan must be in writing and meet other specific requirements.

It is becoming increasingly common to include cybersecurity provisions in the plan document and summary plan description (SPD) (see Standard Clauses, SPD Language, Actions to Take to Avoid Internet Fraud for Distributions and Loans and SPD Language, Identity Theft and Cybersecurity). Provisions within SPDs provide only communications with beneficiaries about the plan, but their statements do not themselves constitute the terms of the plan (*Cigna Corp. v. Amara*, 563 U.S. 421, 468 (2011)). Procedures that are in SPDs, including cybersecurity procedures, that are consistent with the terms of the plan document should be enforceable and sufficient to reasonably apprise plan participants and beneficiaries of their rights and obligations under the plan (29 U.S.C. § 1022(a)).

Providing cybersecurity procedures and information in SPDs may provide a layer of protection for the plan sponsor and fiduciaries if security breaches do occur. In *Foster v. PPB Industries Inc.*, the US Court of Appeals for the Tenth Circuit reviewed a plaintiff's claim brought under ERISA to recover plan benefits allegedly due to the plaintiff after the plaintiff's ex-wife fraudulently withdrew the plaintiff's entire plan account balance. The court held that the plan administrator's decision to not reimburse the plaintiff for the amount the plaintiff's ex-wife withdrew was not an abuse of discretion. (693 F.3d 1226 (10th Cir. 2012)).

In reaching its decision, the Tenth Circuit relied on the fact that the plan administrator notified participants through the SPD of their ability to access their account information electronically and the procedures regarding PINs. Based on this and other language in the SPD, the Tenth Circuit found that the plaintiff was fully informed of how the plan was allowing the plaintiff access to the plaintiff's money and that someone with the correct user ID and PIN was to be treated as the legal participant for processing withdrawals.

Plan Assets and Cybersecurity

ERISA recognizes a fiduciary duty to protect plan assets, but that definition has not yet been extended to specifically encompass plan data, though case law is developing in this area.

Under ERISA Section 3(42), the term "plan assets" means plan assets as defined by the regulations (29 U.S.C. § 1002(42)). The regulations define two broad categories of plan assets, which are:

- **Plan investments.** When a plan invests in another entity, the plan's assets include its investment but do not, solely by reason of this investment, include any of the underlying assets of the entity (29 C.F.R. § 2510.3-101(a)(2)).
- **Participant contributions.** Participant contributions are amounts that a participant or beneficiary pays to an employer or that a participant has withheld from the participant's wages by an employer (29 C.F.R. § 2510.3-102(a)(1)).

ERISA Section 406 prohibits a plan from engaging in a transaction where the plan knows that this transaction involves a transfer to or use by or for the benefit of a party in interest of any assets of the plan (29 U.S.C. § 1106). Under ERISA Section 406, if the definition of a plan asset includes the actual data and information that plans maintain, fiduciaries may be liable for a prohibited transaction related to any misuse or self-dealing regarding these assets or security breaches resulting from the transfer of this data between the plan sponsor and other plan parties in interest.

The regulations do not suggest that PII, account information, and other data that plans maintain fall within the definition of a plan asset.

Plan Asset Case Law

Case law is emerging that may complete the link between treating participant information and data as a plan asset for which the ERISA fiduciary duties and responsibilities apply. These developments may further complicate prohibited transaction analyses.

One court has noted that there is not a single case in which a court has held that releasing confidential information or allowing someone to use confidential information constitutes a breach of fiduciary duty under ERISA or that this information is a plan asset in a prohibited transaction (*Divane v. Nw. Univ.*, 2018 WL 2388118, at *12 (N.D. Ill. May 25, 2018), *aff'd on other grounds*, 953 F.3d 980 (7th Cir. 2020)).

Plan participants are raising fiduciary breach claims when their data is disclosed to third parties for product marketing based on arguments that their data is a valuable plan asset to be used for their exclusive benefit to provide plan benefits.

In *Cassell v. Vanderbilt University*, the plaintiffs brought both breach of fiduciary duty claims and claims for violations of prohibited transaction rules, alleging that the plan allowed plan service providers to use their positions as recordkeepers to obtain access to participants, learning their ages, length of employment, contact information, account sizes, and investment choices, and used that information in marketing lucrative investment products and wealth management services to participants as they neared retirement and before retirement. The case settled before progressing through motion practice, but the settlement contained one provision requiring the plan's current recordkeeper to refrain from using information about plan participants acquired in the course of providing recordkeeping services to the plan to market or sell products or services unrelated to the plan unless a request for these products or services is initiated by a plan participant (285 F. Supp. 3d 1056 (M.D. Tenn. 2018)).

More recently, in *Harmon v. Shell Oil Company*, the US District Court for the Southern District of Texas determined that it was unable to conclude that participant data is a plan asset under ERISA and granted a motion to dismiss the case (2021 WL 1232694 (S.D. Tex. Mar. 30, 2021)).

Cases are continuing to emerge regarding the use of participant confidential information to market financial products and services outside the benefit plan and are likely to evolve in determining whether participant information and data is a plan asset to which ERISA fiduciary responsibilities may extend.

Plan sponsors and fiduciaries should:

- Recognize these developments.
- Take prudent steps to manage and protect participant data.
- Ensure that the data is used for the exclusive interest of participants.
- Monitor state requirements related to notifications to employees concerning use of their data and determine the applicability of these requirements to plan participants (for example, there are notice requirements under the California Consumer Privacy Act (CCPA) of 2018 and California Privacy Rights Act (CPRA) of 2020 regarding use of employee data and sensitive personal information).

Potential Claims of Fiduciary Liability Under ERISA for Retirement Plan Cybersecurity Breaches

A cybersecurity breach of participant data or account assets under a retirement plan can expose plan sponsors and fiduciaries to a potential breach of fiduciary duty litigation risk as well as other potential liabilities.

In the few cases that have been brought to date, participants and beneficiaries have asserted a variety of claims, including:

- Claims for breach of fiduciary duty under ERISA.
- Claims for denial of benefits under ERISA.
- Various state law claims (for example, breach of state privacy laws, breach of contract, unjust enrichment, and negligence).

This is an evolving area of law, and many cases are unreported or settled. By being aware of the types of claims that can be brought, plan sponsors and fiduciaries can be better prepared to develop prudent practices and protect against this type of litigation and the potentially vast damages.

ERISA Section 502(a)(2)

ERISA Section 502(a)(2) provides a cause of action for breach of fiduciary duty for "appropriate relief" under ERISA Section 409, which imposes obligations on fiduciaries involving the "proper management, administration, and investment of fund assets" (29 U.S.C. §§ 1132(a)(2) and 1109). A civil action may be brought by participants, beneficiaries, plan fiduciaries, and the Department of Labor (DOL) against a fiduciary for a breach of its fiduciary duties under ERISA Section 502(a)(2).

ERISA Section 409:

- Permits the plan to recover any losses resulting from a breach of fiduciary duty.
- Provides that a fiduciary is personally liable for:
  - losses caused to the plan;
  - restoration to the plan of any profits that the fiduciary made by using plan assets; and
  - other equitable or remedial relief as a court may deem appropriate, including removal of the fiduciary.

(29 U.S.C. § 1109 and see Practice Note, ERISA Litigation: Causes of Action and Remedies Under ERISA Section 502 for Benefit and Fiduciary Breach Claims.)

In *Massachusetts Mutual Life Insurance Co. v. Russell*, the US Supreme Court held that ERISA Section 502(a)(2) only provides relief that inures to the benefit of the plan as a whole (473 U.S. 134 (1985)). However, in *LaRue v. DeWolff, Boberg & Associates*, the US Supreme Court noted that while ERISA Section 502(a)(2) does not provide a remedy for individual injuries distinct from plan injuries, it does authorize recovery for fiduciary breaches that impair the value of plan assets in a participant's individual account (552 U.S. 248 (2008)). Therefore, there is an avenue to relief under ERISA Section 502(a)(2) for harm to an individual account in a defined contribution plan.

Regarding cybersecurity, ERISA Section 502(a)(2) claims have been brought in the context of fraudulent plan account distributions. For example, in *Leventhal v. MandMarblestone Group, LLC*, the plaintiff brought a claim against the defendant after the plaintiff's 401(k) account was fraudulently reduced from almost $400,000 to $0 (2019 WL 1953247 (E.D. Pa. May 2, 2019)). The plaintiff alleged that the defendant:

- Improperly distributed the funds to a bank account that was never authorized by the plaintiff and that the withdrawal of this substantial amount of money was never authenticated with forms or a signature from the plaintiff.
- Did not implement its procedures in notifying the plaintiff of these strange requests or to verify the authenticity of these requests.

Addressing the defendant's motion to dismiss for failure to state a claim, the court found that the plaintiffs sufficiently pleaded a breach of duty by alleging that the defendant failed to act with the requisite prudence and diligence where the defendants saw the peculiar nature and high frequency of the withdrawal requests that were to be distributed to a new bank account but failed to alert the plaintiffs or verify the requests. The court also relied on the fact that the defendant failed to implement the typical procedures and safeguards used to notify the plaintiffs of the strange requests and to verify the requests. The case is currently pending in the US District Court for the Eastern District of Pennsylvania. In a more recent development, the court also permitted the plan administrator to assert counterclaims against co-fiduciaries for contribution and indemnification, alleging their own carelessness (*Leventhal v. The MandMarblestone Group LLC*, 2020 WL 2745740 (E.D. Pa. May 27, 2020)).

Similarly, the plaintiff in *Berman v. Estee Lauder* brought claims against the defendants alleging that the plan had allowed the plaintiff's $99,000 401(k) account to be fraudulently distributed to various bank accounts without the plaintiff's authorization. The plaintiff alleged that the defendants breached their fiduciary duty of loyalty and prudence by:

- Allowing the plan to make unauthorized distributions of plan assets.
- Failing to confirm authorization for distributions with the plan participant before making distributions.
- Failing to provide timely notice of distributions to the plan participant by telephone or email.
- Failing to establish distribution processes to safeguard plan assets against unauthorized withdrawals.
- Failing to monitor other fiduciaries' distributions processes.

(Complaint (ERISA), *Berman v. Estee Lauder*, No. 3:19-CV-06489 (N.D. Cal. Oct. 9, 2019) (case settled in March 2020).)

In *Bartnett v. Abbott Laboratories*, the plaintiffs' complaint asserted breach of fiduciary duty claims against the plan sponsor, other plan administrators, and recordkeepers seeking to recover $245,000 that was depleted from the plaintiff's retirement account in alleged unauthorized distributions by an impersonator fraudulently accessing the plaintiff's online account. The court granted in part and denied in part the defendants' motions to dismiss the complaint. (*Bartnett v. Abbott Labs.*, 492 F. Supp. 3d 787, 802 (N.D. Ill. 2020).) The plaintiff later filed her first amended complaint, and the court granted the defendants' motion to dismiss the amended complaint (*Bartnett v. Abbott Labs.*, 2021 WL 428820 (N.D. Ill. Feb. 8, 2021)).

These recent cases allege that fiduciaries breach their duty by failing to establish and maintain processes to safeguard plan assets. Aligned with the court's reasoning in *Leventhal* and the EBSA Cybersecurity Guidance, when plan fiduciaries establish procedures to safeguard participants' data and mitigate risks, and abide by those procedures, they can provide a better safeguard against liability for these claims.

Claims for Appropriate Equitable Relief Under 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 Section 502(a)(3) (29 U.S.C. § 1132(a)(3)) where the remedy for a successful claim is equitable relief for individual harm. The DOL may sue for similar relief under ERISA Section 502(a)(5) (29 U.S.C. § 1132(a)(5)).

In *Cigna v. Amara*, the US Supreme Court discussed surcharge as another type of equitable relief that may be available in fiduciary breach cases. Surcharge is a remedy that arises in cases involving a breach of trust. To be granted a surcharge, the Court found that a plaintiff must show that:

- There was a breach of trust by a fiduciary.
- There was actual harm suffered by the beneficiary.
- The breach caused the harm.

This provides a framework for a type of make-whole relief where a plaintiff can show breach of duty, causation, and resulting harm.

A fiduciary may bring suit under ERISA Section 502(a)(3) to enjoin any act or practice that violates ERISA or the terms of the plan or to obtain other appropriate equitable relief to either:

- Redress these violations.
- Enforce any provisions of ERISA or the terms of the plan.

A plan or plan sponsor may bring a suit against a service provider under ERISA Section 502(a)(3) to enjoin them from a certain practice regarding a plan (for example, sending data to a particular cloud provider). Claims under state law may also be available against service providers that are not ERISA fiduciaries.

ERISA Section 502(a)(3) is referred to as the catchall provision and normally provides relief for injuries not adequately remedied elsewhere under ERISA Section 502 (*Varity Corp. v. Howe*, 516 U.S. 489, 515 (1996)).

To bring a claim under this section, a plaintiff generally must prove that both:

- There is a remediable wrong (for example, that the plaintiff seeks relief to redress a violation of ERISA or the terms of the plan).
- The relief sought is appropriate equitable relief.

(See, for example, *Gabriel v. Alaska Elec. Pension Fund*, 773 F.3d 945, 954 (9th Cir. 2014) and *Mertens v. Hewitt Assocs.*, 508 U.S. 248, 256 (1993).)

From the limited number of cases that have been brought, it is apparent that these types of claims generally are not alleged by participants and beneficiaries when a cybersecurity breach occurs, opting instead

for clams that allow for compensatory damages (see *Leventhal v. MandMarblestone Grp., LLC*, 2019 WL 1953247 (E.D. Pa. May 2, 2019); Complaint (ERISA), *Berman v. Estee Lauder*, No. 3:19-CV-06489 (N.D. Cal. Oct. 9, 2019) (seeking to recoup $99,000 stolen from 401(k) account)). However, this section may provide relief to participants and beneficiaries where the damages are not so concrete.

In *Cassell v. Vanderbilt*, the plaintiffs alleged that the plan's recordkeepers used:

- Their positions as recordkeepers to obtain access to participant information, learning their ages, length of employment, contact information, account sizes, and investment choices.
- That information in marketing lucrative investment products and wealth management services to participants as they neared retirement and before retirement.

The settlement agreement that the parties reached addressed these concerns by obligating the plan sponsor to refrain from using information about plan participants acquired in the course of providing recordkeeping services to the plan to market or sell products or services unrelated to the plan unless a request for these products or services is initiated by a plan participant.

Another potential example can arise where the data stolen includes the participant's social security number, date of birth, home address, email address, bank account information, personal financial information, spousal information, or child and dependent information,. Instead of depleting the participant's 401(k) account, the hacker uses the information to impersonate that individual, causing damage to the individual's credit score and racking up thousands of dollars in debt. This identity theft causes irreparable harm to the participant but is difficult to quantify. It remains to be seen whether the equitable relief available under Section 502(a)(3) may be invoked.

Claims for Benefits Under the Plan Terms Under Section 502(a)(1)(B)

Individual benefit claims are brought under ERISA Section 502(a)(1)(B) (29 U.S.C. § 1132(a)(1)(B)), which allows participants and beneficiaries to bring a civil cause of action to recover benefits due under a plan to either:

- Enforce rights under the terms of the plan.
- Clarify future rights to benefits under the terms of the plan.

An ERISA plan can impose a lawsuit-filing deadline if it is reasonable.

These claims require a plaintiff to show that they:

- Properly made a claim for benefits.
- Exhausted the plan administrative appeals process (if raised as a defense).
- Are entitled to a particular benefit under the plan's terms.
- Were denied that benefit.

As characterized by the US Court of Appeals for the Fifth Circuit, when an individual simply wants what was supposed to have been distributed under the plan, the appropriate remedy is under ERISA Section 502(a)(1)(B) (*Hager v. DBG Partners, Inc.*, 903 F.3d 460, 469 (5th Cir. 2018)).

In *Foster v. PPB Industries Inc.*, the Tenth Circuit upheld a decision in which the plan administrator denied the plaintiff's request for additional benefits on the grounds that:

- The plan had in place all the necessary and proper security measures.
- The benefits were paid under all plan terms and requirements.
- The plaintiff's loss of benefits was due to the plaintiff's own failure to comply with the plan's address change requirements as well as the fraudulent conduct of the plaintiff's ex-spouse.

(693 F.3d 1226 (10th Cir. 2012).)

The plaintiff challenged this determination in the district court, saying the money had been forfeited in violation of ERISA, and demanded from the defendant a distribution of the plaintiff's share of the plan, but the defendants denied this request. The Tenth Circuit relied on the fact that the plan administrator notified the plaintiff and other participants through the SPD of their ability to access their account information electronically and to keep their address information current, as all Plan correspondence was to be mailed to their current address on file and PIN changes and resets are always mailed to the permanent address on file. The Tenth Circuit affirmed that decision, holding that the plan administrator's decision to not reimburse the plaintiff for the amount the plaintiff's ex-wife withdrew was not an abuse of discretion. The Tenth Circuit instead found that the plan administrator safeguarded plan assets as they had already been paid out in the plaintiff's name and to do so again then depletes plan assets. (*Foster*, 693 F.3d 1226.)

Based on the court's ruling in *Foster*, which rested heavily on the facts of that case, a plan may not be liable

to a participant under ERISA Section 502(a)(1)(B) (29 U.S.C. § 1132(a)(1)(B)) for denial of benefits where the plan follows procedures that are communicated to participants and where participants are found not to have followed those procedures.

Other Avenues to Bring Claims

Other avenues to bring claims related to cybersecurity and benefit plans include:

- State law claims (to the extent not preempted by ERISA).
- Breach of contract.
- Unjust enrichment.
- Promissory or 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.

ERISA preemption analysis under ERISA Section 514 (29 U.S.C. § 1144) is a threshold question. Under ERISA Section 514, state laws that relate to ERISA plans are preempted, unless the state law is saved from preemption under the savings clause. While ERISA is designed to provide a single uniform national scheme to administer plans without interference from state law, plan fiduciaries should not assume that ERISA preempts applicable laws related to data privacy and security when addressing cybersecurity of benefit plan data. Data can also be stolen from programs not governed by ERISA (see Practice Note, ERISA Litigation: Preemption of State Laws: Overview).

For complete ERISA preemption to arise, it must be that the individual brought a claim for plan benefits under ERISA Section 502(a) (29 U.S.C. § 1132(a)) and there is no other independent legal duty that is implicated by the defendant's actions.

Other Laws

Plan sponsors and fiduciaries should know the landscape of laws in locations where the organization operates and where participants reside. Consideration should be given to ensure that the employer's organization data security programs are designed in compliance with applicable law, including:

- Required notices of data collection.
- Security standards.
- Breach notification procedures.

Under the current landscape, plan sponsors and fiduciaries should also be mindful of the laws addressing data privacy and security as this area continues to evolve, which may serve as the basis for various areas of litigation and compliance enforcement and penalties. Examples of laws to consider include:

- **Gramm-Leach-Bliley Act of 1999 (GLBA).** 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 (GDPR).** Rules relating to the protection of natural persons regarding the processing of personal data and rules relating to the free movement of personal data. Provides individual data subjects with the right to be forgotten or have the controller erase their personal data.
- **SEC's Regulation S-P.** 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 PHI and security standards to protect the confidentiality, integrity, and availability of electronic PHI. Expands obligations of business associates and contains 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 Federal Trade Commission (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. The FTC also enforces other federal laws relating to consumers' privacy and security.
- **State privacy statutes.** Examples of state privacy statutes include New York's Stop Hacks and Improve Electronic Data Security Act (SHIELD Act) of 2019, CCPA and CPRA.

Department of Labor Initiative

Before the issuance of the EBSA Cybersecurity Guidance, EBSA had been studying and monitoring the issues related to cybersecurity of employee benefit plans. EBSA has been involved in multi-agency investigations and is aware of a multitude of potential cybersecurity threats.

Advisory Council on Employee Welfare and Pension Benefit Plans

In 2011, the Advisory Council on Employee Welfare and Pension Benefit Plans (Council) studied the importance of addressing privacy and security issues regarding employee benefit plan administration. The Council examined concerns about:

- Potential breaches of the technological systems used in the employee benefit industry.
- The misuse of benefit data and PII.
- The effect on all parties sharing, accessing, storing, maintaining, and using PII, including plan sponsors and fiduciaries, trustees, participants, plan administrators, third-party administrators (TPAs), recordkeepers, investment advisors, and other service providers.

The Council recognized several potential areas of vulnerability, including:

- Theft of personal identities and other PII.
- Theft of money from bank accounts, investment funds, and retirement accounts.
- Unsecured or unencrypted data.
- Outdated and low security passwords.
- Hacking into plan administration, service provider, and broker systems.
- Email hoaxes.
- Stolen laptops or data hacked from public computers where participants logged into accounts.

The Council recommended that the DOL provide guidance on the obligation of plan fiduciaries to secure PII and develop educational materials.

The ERISA Advisory Council has asked the DOL to provide guidance on how plan sponsors should evaluate the cybersecurity risks they face for plan data and PII so that it can be properly managed, especially regarding third-party relationships for plan administration. In the 2016 Council Report, Cybersecurity Considerations for Employee Benefits Plans (November 2016), the Council provided insights into best practices and provided sample questions to pose to service providers in RFPs.

Cybersecurity Guidance for Plan Sponsors, Plan Fiduciaries, Recordkeepers, and Plan Participants

In 2021, the EBSA Cybersecurity Guidance was issued, providing plan sponsors, plan fiduciaries, recordkeepers, plan participants, and beneficiaries with best practices for maintaining cybersecurity, including tips on how to protect workers' retirement benefits.

The guidance is in three forms, which are:

- **Tips for Hiring a Service Provider.** Helps plan sponsors and fiduciaries prudently select a service provider with strong cybersecurity practices and monitor their activities.
- **Cybersecurity Program Best Practices.** Assists plan fiduciaries and recordkeepers in their responsibilities to manage cybersecurity risks.
- **Online Security Tips.** Offers plan participants and beneficiaries who check their retirement accounts online basic rules to reduce the risk of fraud and loss.

Other Government and Industry Efforts

Retirement industry groups, such as the Spark Institute and the Financial Services Information Sharing and Analysis Center, joined forces to establish the Retirement Industry Council to share information about new data security threats and strategies for improving security in the retirement market. The SPARK Institute, through its Data Security Oversight Board, also worked to develop standards for recordkeepers to demonstrate the security capabilities of their systems, including through reporting of their system controls.

The SPARK Institute's Data Security Oversight Board developed guidelines in 2020 regarding how recordkeepers can properly communicate with plan administrators and other service providers concerning penetration testing results. Communicating these results is a security risk in and of itself because this communication may potentially pinpoint areas where the organization is weaker or needs improvement. The SPARK Institute has advised that recordkeepers can make representations that they adhere to SPARK data security best practices for penetration testing, which should be inclusive of anywhere that nonpublic information or PII is processed or stored.

Recordkeepers should communicate:

- The types of tests performed.
- The frequency of the tests.
- High level findings.
- Remediations.

Individual states continue to issue rules for handling of employee information and data, which raises ERISA preemption questions regarding their application to employee benefit plan administration. Many US government agencies and state agencies have also issued cybersecurity alerts, notices, and general warnings related to the protection of employee data, consumer data, taxpayer data, and other information, which may be the same information that may be collected by plan sponsors and fiduciaries that may affect employee benefit plan administration. Most of these are guidelines, but they may affect employee benefit plans' policies and best practices.

In February 2019, Congress issued a written request to the US Government Accountability Office (GAO) to examine the cybersecurity of the private retirement system (Congressional Request Letter to GAO), noting that despite various initiatives and forums, the cybersecurity safeguards, risks, and liabilities for plan sponsors and participants remain ill-defined, especially regarding major data breaches or advanced persistent threats.

In its February 2021 report, the GAO further urged the DOL to issue cybersecurity guidance and recommended that the DOL formally state whether it is a fiduciary's responsibility to mitigate cybersecurity risks in defined contribution plans and to establish minimum expectations for addressing cybersecurity risks in defined contribution plans. The DOL agreed with GAO's second recommendation but did not state whether it agreed or disagreed with the first one.

Plan sponsors and fiduciaries must be cognizant of these developments and do their part to mitigate cybersecurity risks, ensure that they have controls in place that service to prevent security breaches of plan participant data and assets and that they have addressed these considerations with service providers. As noted in the Congressional Request Letter to GAO, current law does not address several questions related to cybersecurity, and retirement plans fall within a patchwork of federal and state laws and regulations.

While there is no clear fiduciary mandate under ERISA, the EBSA Cybersecurity Guidance is a step forward in identifying ways plan sponsors and fiduciaries can mitigate cybersecurity risks as part of their duty to carry out their responsibilities prudently and in the best interests of plan participants and beneficiaries. Employers that take the time to develop and follow a benefit plan cybersecurity policy that addresses these issues in a thoughtful manner may be well-positioned to demonstrate prudence and diligence in these efforts and prepared to act if a data breach occurs.

For guidance for plan fiduciaries to develop prudent policies and procedures to secure that information and data, see Practice Note, Best Practices for ERISA Fiduciary Responsibilities and Cybersecurity for Retirement Plans.