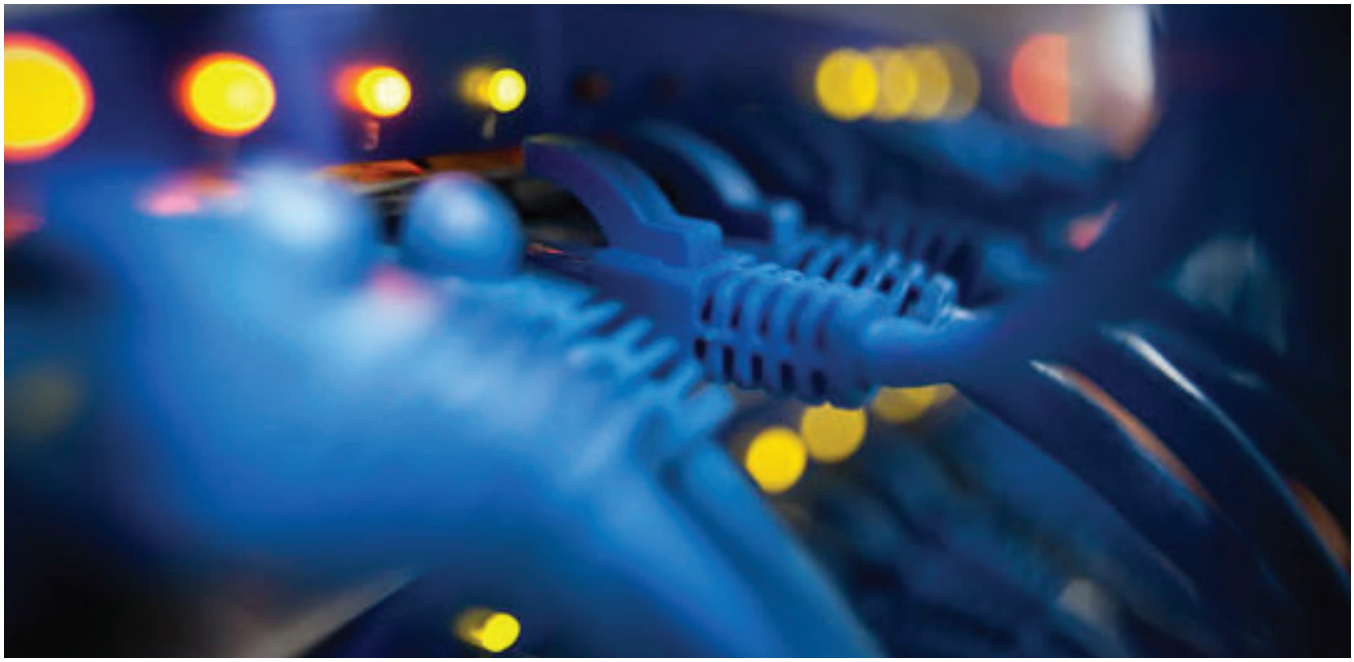
STRADLEY RONON

Fiduciary Governance

Risk&Reward
fiduciarygovernanceblog.com
@FidGovGroup

June 14, 2021

Cybersecurity and Related Legal Risks Come Home to ERISA Plans



ERISA-covered plans have entered the digital world. As the amount of confidential information about plan participants that is stored in multiple information systems, and shared among plan service providers, increases, so, too, do the legal risks. The U.S. Department of Labor (DOL) has now made cybersecurity risk an enforcement priority; the courts have started to wrestle with whether participant data is a "plan asset." Plan sponsors and service providers should brace themselves.

Just this past February, the U.S. Government Accountability Office (GAO) issued a report that highlighted the practice of, and risks related to, sharing personally identifiable information (*e.g.*, a participant's social security number, date of birth and username/password) (PII), and "plan asset data" (*e.g.*, retirement account and bank account numbers) within the plan ecosystem. The plan sponsor's own IT infrastructure may be vulnerable to attack or misuse. Where the plan sponsor outsources plan administrative responsibilities to a service provider, such as recordkeepers, third-party administrators and custodians, participant PII and plan asset data could be exploited if the service provider is hacked or lacks appropriate internal controls.

The report specifically noted that cybersecurity risk comes in many different flavors and from many different sources. The risk could, for example, be in the form of malware, ransomware, privilege abuse, data exfiltration and account takeover. The source of the risk could come from criminal syndicates, hackers and even an organization's own employees.

Thus, the GAO report warned, "[t]he sharing and storing of this information can lead to significant cybersecurity risks for plan sponsors and their service providers, as well as plan participants." Poor risk controls can lead to the leaking of usernames, passwords and social security numbers, which can lead to the unauthorized access of participant accounts, and, fatally, the illicit draining of a participant's retirement savings. The misappropriation of participant PII or plan assets by virtue of a cybersecurity attack may not be expressly addressed in ERISA, but its effect on a participant may indeed result in "the great personal tragedy" Congress sought to prevent in enacting ERISA.[1]

The GAO ultimately made two recommendations: (1) the DOL should formally state whether cybersecurity for ERISA-covered retirement plans is a plan fiduciary responsibility under ERISA; and (2) the DOL should develop and issue guidance that identifies minimum expectations for mitigating cybersecurity risks to plans and the relevant service providers.

A mere two months later, the DOL issued a series of cybersecurity tips and best practices for plan sponsors, service providers and participants. Specifically:

- **Tips for Hiring a Service Provider**, to "[h]elp[] plan sponsors and fiduciaries prudently select a service provider with strong cybersecurity practices and monitor their activities, as ERISA requires."
- **Cybersecurity Program Best Practices**, to "[a]ssist[] plan fiduciaries and recordkeepers in their responsibilities to manage cybersecurity risks."
- **Online Security Tips**, to "[o]ffer[] plan participants and beneficiaries who check their retirement accounts online basic rules to reduce the risk of fraud and loss."

Useful as the tips and practices may be, the big reveal is that the DOL indicated that ERISA's duty of prudence encompasses "an obligation to ensure proper mitigation of cybersecurity risks." This means that a responsible plan fiduciary, when determining whether to hire and retain a service provider, should consider the service provider's cybersecurity risk controls, and should document such consideration as part of its overall evaluation of the service provider.

For more information, please contact:

George Michael Gerstein
Co-Chair, Fiduciary Governance
202.507.5157
ggerstein@stradley.com

The upshot of the DOL's April 2021 cybersecurity tips and best practices is that it puts employers on notice that both the DOL takes this seriously and that plaintiffs could attempt to use this new guidance as a basis for fiduciary duty breach claims. Moreover, service providers can expect detailed questions on cybersecurity in RFPs and RFIs. Plan sponsors will seek more transparency, whereas service providers may be reluctant to divulge too much on their cybersecurity defenses to guard against inadvertently offering up the keys to the castle. The balance of the two will become market practice.

The DOL is ramping up enforcement in this area. Plan sponsors should also gird for class-action lawsuits with allegations of breaches of ERISA's duty of prudence when participant PII or plan asset data is misused. For these reasons, employers and plan service providers should carefully consider the DOL guidance.

A related string of litigation also poses a risk to plan sponsors and service providers. These suits argue that participant PII and plan asset data constitute "plan assets," and that using such data for marketing purposes amounts to a breach of fiduciary duties. Some of these suits have targeted both the plan's sponsor and recordkeeper. So far, the courts have rejected these claims.

In one case,[2] plaintiffs brought an action against the plan sponsor and recordkeeper alleging that participant data (*e.g.*, names, contact info, investment history, *etc.*) constituted "plan assets," and, therefore, the recordkeeper's purported sharing of this information with affiliates to cross-sell non-plan retail financial products to participants amounted to violations of ERISA. In granting the recordkeeper's motion to dismiss, the court ruled that "participant data does not meet the statutory definition of 'plan assets'...."

In a similar case,[3] plaintiffs brought suit against the plan administrator alleging, *inter alia*, breach of fiduciary duty over the plan's recordkeeper access to participant information (*e.g.*, investment choice, account size, *etc.*) and use of that data to market products to the participants. In granting the motion to dismiss, the court stated, "[p]laintiffs cite no case in which a court has held that such information is a plan asset for purposes of ERISA....[t]his Court does not intend to be the first." Moreover, the court rejected the argument that "releasing confidential information or allowing someone to use confidential information constitutes a breach of fiduciary duty under ERISA."

Cybersecurity is quickly becoming an important risk area for ERISA plan sponsors. Protection of participant PII and plan asset data against privilege abuse, account takeovers and other vulnerabilities to a participant's information and account raises the specter for DOL enforcement action and litigation. Service providers should anticipate a greater focus on their cybersecurity measures by plan sponsors and expect that such measures could be an important basis to be hired and retained as a plan service provider. Both employers and plan service providers should also consider whether it is complying with other applicable privacy laws (to the extent such laws are not preempted by ERISA).

---

[1] *Nachman Corp. v. PBGC*, 446 U.S. 359, 374, 100 S. Ct. 1723, 1733, 64 L. Ed. 2d 354, 366 (1980).
[2] *Harmon v. Shell Oil Co.*, No. 3:20-cv-00021, 2021 BL 126207 (S.D. Tex. Mar. 30, 2021)
[3] *Divane v. Northwestern Univ.*, No. 16 C 8157, 2018 BL 186065 (N.D. Ill. May 25, 2018), *aff'd*, 953 F.3d 980 (7th Cir. 2020).