BCLP. Client Intelligent

BenefitsBCLP

ERISA FIDUCIARY OBLIGATIONS EXPANDED TO INCLUDE MITIGATION OF CYBERSECURITY RISKS

Apr 19, 2021

The clouds have been forming on the horizon for years now: from the courts we have seen emerging lines of ERISA litigation asserting fiduciary obligations to protect the privacy rights of participants, and from the regulatory agencies we have heard an acknowledgment of the need for guidance regarding fiduciary responsibility with respect to cybersecurity risks. A call to action for plan fiduciaries came last week from the Department of Labor ("DOL") in the form of new Cybersecurity Guidance for Plan Sponsors, Plan Fiduciaries, Record-Keepers, Plan Participants.

The DOL guidance provides:

1. Tips for Hiring a Service Provider With Strong Cybersecurity Practices
2. Cybersecurity Program Best Practices for plan fiduciaries, record-keepers and other service providers
3. Online Security Tips for participants to help them reduce the risk of fraud and loss to their retirement accounts and report identify theft and cybersecurity incidents

Cybersecurity Governance Programs

Plan fiduciaries who have not yet developed a cybersecurity governance program should do so now, and existing programs should be re-evaluated and updated in light of this guidance. Such cybersecurity governance programs should address all three aspects of the guidance (i.e., development of best practices which include guidelines for hiring service providers and participant education). See Cybersecurity Program Best Practices.

More specifically, the core elements of a strong cybersecurity governance program should include the following:

- Develop, document and regularly monitor and update a formal cybersecurity program
- Conduct annual risk assessments

- Have a reliable annual third party audit of security controls
- Clearly define and assign information security roles and responsibilities
- Have strong access control procedures
- Ensure that any assets or data stored in a cloud or managed by a third party service provider are subject to appropriate security reviews and independent security assessment
- Conduct regular cybersecurity awareness training
- Implement and manage a secure system development life cycle program
- Have an effective business resiliency program addressing business continuity, disaster recovery, and incident response
- Encrypt sensitive data, stored and in transit
- Implement strong technical controls in accordance with best security practice
- Appropriately respond to any past cybersecurity incidents
- Follow tips for hiring a service provider with strong cybersecurity practices. *See Tips for Hiring a Service Provider with Strong Security Practices.*
- Educate participants with respect to online security. *See Online Security Tips.*

Cybersecurity Litigation

The emerging litigation relating to cybersecurity litigation also provides helpful insight. These cases generally follow two lines of claims. The first is that participant data is a plan asset entitled to the same fiduciary protections and prohibited transaction rules applicable to plan funds. Under this theory, the use of participant data for any purpose other than for the exclusive purpose of providing plan benefits would constitute a fiduciary breach. To date, the courts have been split on their acceptance of this theory. While some courts have rejected such theory in the absence of DOL guidance expanding plan asset protection to participant data, there have been several significant court approved settlements suggesting participant data may be viewed as a plan asset. Careful re-evaluation of the use of participant data in light of this litigation trend can offer fiduciaries some protection until more reliable guidance is established. The second line of litigation seeks to impose liability on plan fiduciaries when a participant's benefits are fraudulently withdrawn from their accounts. In these cases, good cybersecurity governance measures, including participant education, have been instrumental in defending such claims.

RELATED PRACTICE AREAS

- Employee Benefits & Executive Compensation

MEET THE TEAM

Lisa A. Van Fleet

St. Louis

lisa.vanfleet@bclplaw.com
+1 314 259 2326
