Checklist

Cybersecurity Preparedness Checklist for Plan Fiduciaries

Elliot D. Raff and Harold J. Ashner, Keightley & Ashner LLP

Bloomberg Law

Cybersecurity Preparedness Checklist for Plan Fiduciaries

Editor's Note: Contributed as an adjunct to the authors' article, "Surviving a DOL Cybersecurity Audit – A Cybersecurity Preparedness Checklist for Plan Fiduciaries."

This checklist was contributed by Elliot D. Raff and Harold J. Ashner, Keightley & Ashner LLP

Fiduciaries should complete the following checklist for each service provider, for example, a payroll provider, 401(k) plan recordkeeper and administrative service provider, and an institutional trustee.

Neither the DOL guidance nor this checklist ranks or assigns relative importance to the questions and practices it describes. To the extent questions in this checklist are answered in the negative, consideration should be given to potential changes in policy, procedures, contract terms and/or monitoring, as appropriate. Answering "yes" to questions provides a degree of assurance but is no guarantee that fiduciary conduct would be considered prudent.

Cybersecurity Preparedness Checklist for Plan Fiduciaries		
	Yes	**No**
Part 1 - At the time the Service Provider was selected:		
Did you either (a) have the expertise necessary to evaluate cybersecurity standards, practices and policies, or (b) obtain internal or third-party cybersecurity expert resources? *In the following questions, "you" refers to you and/or, if applicable, your cybersecurity expert resource.*		
Did you ask for and receive information describing their information security standards, practices, and policies?		
If so, did you compare those standards, practices, and policies:		
To industry standards, practices, and policies?		
To the DOL's Cybersecurity Program Best Practices?		
Did you find out if they use an outside (third-party) auditor to review and validate their cybersecurity?		
Did you ask if they use an outside (third-party) auditor to test their cybersecurity, for example, to conduct penetration testing?		

	Yes	No
Did you search for and review public information concerning any information security incidents and/or any litigation or other legal proceedings?		
Did you ask whether they experienced past security breaches and, if so, what happened and how they responded?		
Did you ask if they had an insurance policy that would cover losses caused by cybersecurity and identity theft breaches?		
If so, did you:		
Determine that the amount of coverage was appropriate under the circumstances?		
Determine that the insurance covers cybersecurity and identity theft breaches by internal and external actors (*e.g.*, employees, contractors, and outside cyberthieves)?		
Did you document the foregoing inquiries and responses?		
Part 2 - Contract Terms		
Does the contract with the Service Provider:		
Require ongoing compliance with specifically-identified cybersecurity and information security standards?		
Give you the right to review audit results demonstrating compliance with the applicable standards?		
Provide that the service provider is responsible for IT security breaches without limit?		
Require notification of security breaches:		
Only if participants in your plan are affected?		
Even if participants in your plan are not affected?		

	Yes	No
Part 3 – Monitoring the Service Provider's Cybersecurity Program		
Do you either: (a) have the expertise necessary to evaluate cybersecurity standards, practices and policies, or (b) use internal or third-party cybersecurity expert resources? *In the following questions, "you" refers to you and/or, if applicable, your cybersecurity expert resource.*		
Have you received periodic reports (at least annually) from a third-party auditor concerning the Service Provider's cybersecurity program?		
Do you receive periodic reports from the Service Provider concerning or describing:		
Security assessments relating to PII and/or plan asset data stored in a cloud or managed by the Service Provider?		
Its secure system development life cycle (SDLC) program?		
Its security technical controls, including firewalls, antivirus software, and data backup?		
Its cybersecurity capabilities and procedures?		
Its policies and procedures for collecting, storing, archiving, deleting, anonymizing, warehousing, and sharing data?		
Permitted uses of data by the sponsor of the plan or by any of the plan's service providers, including, but not limited to, all uses of data for the direct or indirect purpose of cross-selling or marketing products and services?		

