APPENDIX

Cybersecurity Preparedness Checklist for Plan Fiduciaries

Fiduciaries should complete the following checklist[6] 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

Part 1 — At the time the Service Provider was selected:	
Did you either (a) have the expertisenecessary 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.*	YES NO
Did you ask for and receive information describing their information security standards, practices, and policies?	YES NO
If so, did you compare those standards, practices, and policies:	
To industry standards, practices and policies?	YES NO
To the DOL's Cybersecurity program Best Practices?	YES NO
Did you find out if they use an outside (third-party) auditor to review and validate their cybersecurity?	YES NO
Did you ask if they use an outside (third-party) auditor to test their cyersecurity, 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?	YES NO
Did you ask whether they experienced past security breaches and, if so, what happened and how they responded?	YES NO
Did you ask if they had an insurance policy that would cover losses caused by cybersecurity and identity theft breaches?	YES NO
If so, did you: Determine that the amount of coverage was appropriate under the circumstances?	YES NO
Determine that the insurance covers cybersecurity and identity theft breaches by internal and external actors (e.g., employees, contractors, and outside cyberthieves)?	YES NO
Did you document the foregoing inquiries and responses?	YES NO
Part 2 — Contract Terms	
Does the contract with the Service Provider:	
Require ongoing compliance with specifically-identified cybersecurity and information security standards?	YES NO
Give you the right to review audit results demonstrating compliance with the applicable standards?	YES NO
Provide that the service proider is responsible for IT security breaches without limit?	YES NO
Require notification of security breaches:	
Only if participants in your plan are affected?	YES NO
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.*	YES NO
Have you received periodic reports (at least annually) from a third-party auditor concerning the Service Provider's cybersecurity program?	YES NO
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?	YES NO
Its secure system development life cycle (SDLC) program?	YES NO
Its security technical controls, Including firewalls, antivirus software, and data backup?	YES NO
Its cybersecurity capabilities and procedures?	YES NO
Its policies and procedures for collecting, storing, archiving, deleting, anonymizing, warehousing, and sharing data?	YES NO
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 ndirect purpose of cross-selling or marketing products and services?	YES NO

Disclaimer: This checklist is for informational purposes only, and should not be construed as legal advice, which has to be addressed to particular facts and circumstances involved in any given situation. Review or use of this checklist does not create an attorney-client relationship with the authors or publisher. Please consult with an attorney with the appropriate level of experience if you have any questions.

[6] Contributed by Elliot D. Raff, McDonald & Hopkins LLC, and Harold J. Ashner, Keightley & Ashner LLP.

ISSN 0747 -8607