Mercer

welcome to brighter

Cybersecurity checklist for DC plan sponsors

In April 2021, the Department of Labor (DOL) released guidance for defined contribution (DC) plan sponsors, fiduciaries and participants regarding the protection of retirement benefits and personal information against cyber threats. The DOL issued its guidance in response to a report from the General Accounting Office released in March that recommended the DOL clarify fiduciary responsibilities regarding cybersecurity. Although the DOL guidance stopped short of addressing specific fiduciary responsibilities, the DOL has begun a new audit process for retirement plans on cybersecurity.

Administering retirement plans includes the handling of personally identifiable information (PII) by plan sponsors and their service providers. Beyond the risk of DOL audit, ineffective security controls can lead to the loss or unauthorized disclosure of PII or plan asset data — or worse, the theft of retirement savings of individual participants. The FBI receives 3,000 to 4,000 cybersecurity complaints daily, up from 1,000 per day before the COVID-19 pandemic.

Cybercrime costs are predicted to reach $6 trillion annually in 2021.[1]

Mercer believes there are steps plan sponsors and fiduciary committees can and should take now to begin to codify their own monitoring and communication efforts.

1. **Consider establishing a policy regarding cybersecurity monitoring**, or amend the committee charter to define the oversight that will be conducted and the responsible parties within the organization. Confirm that the committee agrees to perform on an ongoing basis any specific actions identified, including documenting the activity and its completion. Regular review of any such policy and committee charter is also important.

2. **Regularly communicate with participants regarding best practices[2] for protecting their accounts** from cyber threats and fraud. This should include enrollment communication and annual communications specifically on this topic. Use your recordkeeper as a resource to expand the messaging. For years, sponsors have directed participants to take a "set it and forget it" approach to their accounts, but active participants are more likely to identify a one-off breach of an account on a timely basis. Document communication activity within sponsor records.

3. **Review the annual audit report issued on the plan recordkeeper's systems and processes**, identify any relevant findings impacting the plan and help

[1] Marsh McLennan. *MMC Cyber Handbook 2021*.

[2] United States Department of Labor, Employee Benefits Security Administration. "Cybersecurity Program Best Practices," available at https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/best-practices.pdf.

ensure that changes have been implemented to address shortcomings. To the extent that committee or internal company resources do not have expertise in this area, engage with an external resource to support the review process. Monitor recurring or significant issues to determine whether to take action on finding an alternative provider. Document audit activity within sponsor and committee records.

4. **Identify any third parties or advisors that have access to PII** or participant financial information through the recordkeeper, and determine what ongoing review of their practices should be conducted. Many recordkeepers outsource statement mailings or communications support that can require the sharing of participant data with third parties.

5. **Understand the fraud policy offered by the recordkeeper**, and monitor ongoing changes to the policy by requesting at least annual updates. Although most recordkeepers are willing to make participants whole for losses incurred through no fault of the participant, some have begun to add stipulations regarding actions that the participant (or the sponsor) must take to be eligible. Confirm that the recordkeeper's fraud policy extends to any contracted third parties.

6. **Review the contract with the recordkeeper** to help ensure it aligns with your organization's expectations on:

    a. Use of participant data, particularly regarding services outside the qualified plan

    b. Financial commitments to reimburse participants if account breaches occur and duration of such commitments

    c. Timely notifications to you as plan sponsor regarding data security or fraud activity impacting your participants or systems

    d. Oversight of third parties contracted by the recordkeeper

    e. Level of support provided for the annual review of cyber practices and corresponding service level agreements

    Engage an external expert to assist with contract review to ensure industry standards are being considered.

7. **Conduct annual meetings between the recordkeeper and the committee regarding cybersecurity**, and include internal experts. Share with the committee materials prepared internally or externally reviewing the recordkeeper's capabilities, and reflect the due diligence undertaken in meeting minutes.

8. When evaluating alternative recordkeepers, **include cybersecurity and fraud prevention questions in any requests for proposal issued**, and consider responses to those questions in the evaluation and selection process. To the extent that external parties are part of the service delivery (external custodians, partners for nonqualified plan services, etc.), confirm that all organizations are evaluated.

9. **Use interim fee benchmarking projects to gather insight into marketplace practices**, and negotiate contractual changes or service enhancements where appropriate. Keeping abreast of changes in the marketplace is necessary to verify whether the incumbent remains current and preferably market leading.

10. **Engage internal or external resources as appropriate.** Committee members typically are not cybersecurity professionals or DC plan specialists; leverage internal IT expertise and/or external resources as appropriate to review recordkeeper capabilities and contractual commitments. Recognizing that IT professionals do not necessarily have expertise in DC plan administration, consider whether an education session for the IT team would be helpful.

We expect cybersecurity to continue to evolve and to be a mainstay of DC plan management and administration. The DOL may yet clarify the fiduciary responsibilities associated with cybersecurity, but until then, these are the actions plan sponsors and committees should take.

Important notices

References to Mercer shall be construed to include Mercer LLC and/or its associated companies.

Mercer does not provide tax or legal advice. You should contact your tax advisor, accountant and/or attorney before making any decisions with tax or legal implications.

This does not constitute an offer to purchase or sell any securities.

The findings, ratings and/or opinions expressed herein are the intellectual property of Mercer and are subject to change without notice. They are not intended to convey any guarantees as to the future performance of the investment products, asset classes or capital markets discussed.

For Mercer's conflict of interest disclosures, contact your Mercer representative or see http://www.mercer.com/conflictsofinterest.

This does not contain investment advice relating to your particular circumstances. No investment decision should be made based on this information without first obtaining appropriate professional advice and considering your circumstances. Mercer provides recommendations based on the particular client's circumstances, investment objectives and needs. As such, investment results will vary and actual results may differ materially.

Information contained herein may have been obtained from a range of third-party sources. Although the information is believed to be reliable, Mercer has not sought to verify it independently. As such, Mercer makes no representations or warranties as to the accuracy of the information presented and takes no responsibility or liability (including for indirect, consequential or incidental damages) for any error, omission or inaccuracy in the data supplied by any third party.

Investment management and advisory services for US clients are provided by Mercer Investments LLC (Mercer Investments). Mercer Investments LLC is registered to do business as "Mercer Investment Advisers LLC" in the following states: Arizona, California, Florida, Illinois, Kentucky, New Jersey, North Carolina, Oklahoma, Pennsylvania, Texas and West Virginia; as "Mercer Investments LLC (Delaware)" in Georgia; as "Mercer Investments LLC of Delaware" in Louisiana; and "Mercer Investments LLC, a limited liability company of Delaware" in Oregon. Mercer Investments LLC is a federally registered investment adviser under the Investment Advisers Act of 1940, as amended. Registration as an investment adviser does not imply a certain level of skill or training. The oral and written communications of an adviser provide you with information about which you determine to hire or retain an adviser. Mercer Investments' Form ADV Parts 2A and 2B can be obtained by written request directed to: Compliance Department, Mercer Investments, 99 High Street, Boston, MA 02110.

A business of Marsh McLennan

6012272-WE