Defined Contribution Institutional Investment Association

Navigating Participant Data Cyberthreats

A Guide for Plan Sponsors

TAKE ACTION CHECKLIST

To help plan sponsors protect both participants and plan fiduciaries in the fight against cybercrime, the following checklist offers some protective action steps to consider, along with links to additional resources.

☐ **Review and follow the DOL's updated 2024 cybersecurity guidance**

Department of Labor: Cybersecurity Guidance Update, September 2024

- Cybersecurity Program Best Practices (Service Providers) 2024
- Tips for Hiring a Service Provider with Strong Cybersecurity Practices 2024
- Online Security Tips (for participants) 2024

☐ **Use a framework for evaluating cybersecurity risks, especially for reviewing and overseeing vendors/service providers**

- Service Organization Control Type 2 (known as SOC 2) by the American Institute of Certified Public Accountants (AICPA).
- The NIST Cybersecurity Framework (CSF) 2.0 (January 2024) by the National Institute of Standards and Technology (NIST), U.S. Commerce Dept.

SPARK Institute: Cybersecurity & Fraud Resources

- SPARK Data Security Industry Best Practice Standards Release 3.0 (January 30, 2024)
- RRC Progress Brief – SPARK Phase Two: Data, Privacy Sensitivities, Solutions, and Guardrails, September 2023
- RRC and SPARK Study: Understanding Data Privacy Sensitivities Across the DC Industry, August 2023
- Plan Sponsor and Advisor Guide to Cybersecurity, October 2022

☐ **Implement, document, and regularly review the retirement plan's cybersecurity policy,** or amend the committee charter

- Leverage the broader organization's existing cybersecurity programs, tools, and protocols as applicable; for example, public companies must disclose information about their processes for identifying, assessing, and managing cybersecurity risks, including the role of management and the board of directors in oversight. SEC.gov | SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies.
- *Plansponsor*, "What Is a Proper Cybersecurity Policy for a Retirement Plan?" January 27, 2025.

☐ **Discuss cybersecurity and data risk in committee meetings**

It may be appropriate to include cybersecurity reviews as part of the ongoing plan fiduciary processes, including committee meetings. Committee cybersecurity oversight can include seeking improved cybersecurity protection terms in contract negotiations, documenting oversight committee discussions and actions taken, and including the organization's chief information security officer (CISO) or appropriate proxy in committee discussions.

- CISA (U.S. Cybersecurity & Infrastructure Security Agency) offers free cybersecurity assessments for public and private sectors at cisa.gov.
- Mercer, Cybersecurity Checklist for Plan Sponsors, 2024 offers a 10-point checklist to help plan sponsors take appropriate precautions to mitigate risk from both internal and external cybersecurity threats.
- Planadviser, "Cybersecurity Best Practices for Retirement Plans," September 3, 2024.