Morgan Stanley

Helping to Protect Retirement Participants Across Service Providers

It's estimated that there are approximately 126 million eligible retirement plan participants in the U.S., holding assets of over $8 trillion, in ERISA-governed retirement plans.[1, 2, 3]

As a result, without sufficient protections and protocols in place, participants and their assets may be at risk from cybersecurity threats. The Department of Labor (DOL) recently published guidance regarding best practices to help plan sponsors, plan fiduciaries, service providers, and plan participants maintain a prudent cybersecurity program within the retirement plan framework. In its guidance, the DOL notes that qualified retirement plans are prime targets for cyber attackers. And, as cybercrime continues to evolve and increase, with an estimated cost of $23.84 trillion globally by 2027, or 35% increase since 2022, the DOL will likely continue its effort to evaluate these practices and offer further guidance and regulations.[4]

Given the backdrop of a corporate retirement industry that requires access to sensitive plan participant data, guidance by the DOL and the importance of plan fiduciaries remaining compliant to the DOL, this piece illustrates how Morgan Stanley helps protect plan participant data through cybersecurity vis-à-vis DOL guidance and considerations to handling while ensuring its security and integrity.

DOL Cybersecurity Guidance

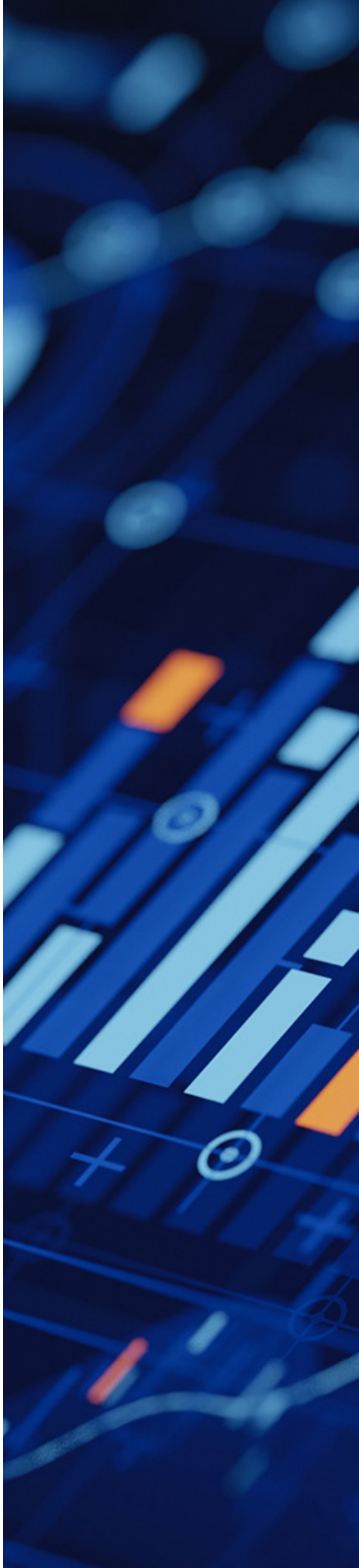
The DOL guidance provides the following best practices for retirement service providers to promote a strong cybersecurity infrastructure:

- Implement a formal, well-documented cybersecurity program that outlines safeguards for IT infrastructure and retirement data from internal and external threats
- Institute formal and effective policies and procedures requiring annual risk assessments and review by a third-party auditor
- Manage cybersecurity programs at the senior executive level
- Service provider users/employees should be subject to strong access control procedures.
- Conduct annual cyber awareness training for employees
- Establish a secure system development lifecycle program, a business resilience program, encryption of sensitive data while stored and in transit and technical controls (i.e., in hardware, software, or firmware)

As the DOL notes, risk assessments for participant data stored in a cloud environment or managed by a third-party service provider are crucial. According to the DOL, for a cybersecurity program to be effective and for accountability, it must be managed at the senior executive level, such as by a chief information security officer (CSIO).

Additionally, service provider users/employees should be subject to strong access control procedures to make sure that only the appropriate individuals have the authorization to access sensitive retirement plan information. This approach would allow a service provider to confirm that its activity is consistent with its cybersecurity program and that any unauthorized use or access of confidential data is detected. The DOL stresses how employees are often an organization's weakest link for cybersecurity. To minimize the impact of the human element in potential security breaches, a service provider's cybersecurity program should include annual cyber awareness training.

The guidance also includes various recommendations for a secure system development lifecycle program, a business resilience program, encryption of sensitive data while stored and in transit, technical controls (i.e., security solutions through mechanisms in the hardware, software, or firmware of a system) in accordance with best security practices, and appropriate responses to any past cybersecurity breaches.



Recordkeeping Partners

One of the most recognizable of qualified retirement plan service providers is the recordkeeper. A recordkeeper is the bookkeeper of a qualified retirement plan. They maintain records of which participants are in the plan and the investments that participants own within the qualified retirement plan wrapper. Companies share participant data directly with these recordkeepers and in turn, participant data is shared by the recordkeeper with Morgan Stanley to service the plan, deliver financial education to plan participants, and provide investment guidance to plans in accordance with fiduciary standards.

Morgan Stanley has partnership agreements with the following recordkeepers:.

- Empower
- Vestwell
- ADP
- John Hancock
- Lincoln
- T. Rowe Price
- Ascensus
- American Funds
- Nationwide
- Paychex
- Principal
- Transamerica
- Voya

Data Security Controls

To deliver on safeguarding client data through our partner recordkeepers, Morgan Stanley has the following measures in place.

Information Security at Partner Recordkeepers

All recordkeeping partners are subject to risk assessments conducted by Morgan Stanley of third-party suppliers. These assessments include an evaluation of cybersecurity and information security controls.

Data Sharing Between Partner Recordkeepers and Morgan Stanley

Partner recordkeepers share participant data daily with Morgan Stanley via a Secure File Transfer Protocol (SFTP) feed.

Morgan Stanley Financial Advisors then access participant data through Morgan Stanley's internal Corporate Retirement Portal. Through the Corporate Retirement Portal, Morgan Stanley Financial Advisors have access to a comprehensive view of their retirement plan books of business and the ability to send targeted participant email communications directly from the Portal, based on the ingestion of recordkeeper data. The Portal ensures that the Firms' corporate retirement clients' data is transferred securely to Morgan Stanley, with proper controls in place and in accordance with the DOL's Cybersecurity Guidance. Access to the Portal , a "single front door," and data contained therein is subject to Morgan Stanley's identity and assessment management controls. Users must submit a request that is reviewed and approved by designated individuals. Access is revoked when access is no longer required, or when an employee is terminated.

Protection of Data Within the Morgan Stanley Environment

CYBERSECURITY

Morgan Stanley makes a significant annual investment in cybersecurity so we can be on guard 24/7, 365 days a year. Our "Defense in Depth" strategy is rooted in defending our most critical systems with multi-layered controls. We utilize strong encryption protocols, continuous monitoring of system access and data movement, and in-house and independent testing for cyber vulnerabilities.

DATA LOSS PREVENTION

Morgan Stanley has deployed multiple mechanisms designed to prevent and detect data leakage. This method includes leveraging technologies to monitoring outbound emails and web uploads for sensitive data elements such as client Personally Identifiable Information (PII) to block unauthorized external data sharing.

The Morgan Stanley Approach

While Morgan Stanley is not a 401(k) recordkeeper, the data security practices outlined above result in a provider-agnostic model whereby Financial Advisors can provide investment management and participant education services while instilling confidence in the secondary housing of participant data.

Morgan Stanley is a firm of over 80,000 employees across 32 countries and can deploy robust risk, technology, and cybersecurity infrastructure to corporate retirement clients regardless of plan AUM or number of participants. As a result, virtually any size plan can benefit from Morgan Stanley's corporate retirement services and cybersecurity infrastructure.

Contact your Financial Advisor if you have additional questions about Morgan Stanley's commitment to keeping sensitive data safe.

[1] ERISA refers to the Employee Retirement Income Security Act of 1974 (ERISA) is a federal law that sets minimum standards for most voluntarily established retirement and health plans in private industry to provide protection for individuals in these plans. These plans allow individuals to accumulate tax-advantaged retirement savings and maintain significant amounts of highly sensitive personal and financial data.

[2] https://crsreports.congress.gov/product/pdf/R/R47699

[3] https://pensionrights.org/resource/how-many-american-workers-participate-in-workplace-retirement-plans/

[4] https://www.imf.org/en/Publications/GFSR/Issues/2024/04/16/global-financialstability-report-april-2024?cid=bl-com-SM2024-GFSREA2024001

CRC 3780859 08/2024