Tips for Complying with DOL's Retirement Plan Cybersecurity Guidance

Anton Janik, Jr.
ajanik@mwlaw.com
(501) 688.8888

05/24/2021

”Not if, but when" is a phrase commonly used to describe data breach risk. Holding just under $11 trillion in assets, employer-sponsored retirement plans are a particularly enticing target for cybercriminals. Through audits and best practice guidance, the Department of Labor (DOL) is encouraging retirement plan sponsors to pay attention to managing cybersecurity risk.

Recognizing that businesses often outsource retirement plan administration, the DOL recently released cybersecurity guidance for plan sponsors, including tips for hiring a service provider with strong cybersecurity practices. Here we provide context about typical retirement plan breaches and offer additional insight on the DOL's best practice guidance.

Retirement Data Breaches Are Unique

Although data breaches are thought of as complex operations executed by coordinated hacking groups, retirement plan breaches are often more elementary. Individual "bad actors" with access to retirement plan information can easily find and exploit system or process vulnerabilities to drain retirement accounts.

The recent *Bartnett v. Abbott Laboratories* case illustrates a typical example: Retired Abbott Labs employee Heide Bartnett's online 401(k) account was accessed by an impostor through the "forgot password" feature using Bartnett's date of birth and the last four digits of her Social Security number. Posing as Bartnett, the impostor called the retirement plan administrator several times, gaining additional confidential information about the retiree from call center employees and eventually succeeding in stealing more than $240,000 from her accounts.

Bartnett sued her former employer, the retirement plan and the third-party vendor for breach of fiduciary duty and other claims under Illinois law.

How can HR managers protect their retirement plan participants from a similar fate and their company from fiduciary-breach claims? The DOL's cybersecurity guidance provides a good starting point. The following tips, intended to be read in conjunction with DOL's guidance, provide additional insight to assist HR managers in putting appropriate protections in place.

Leverage a Contract Renewal

Contract terms should be reviewed at renewal to ensure a vendor's contractual obligations related to data security are clear, ongoing and aligned with the DOL's best practice guidance, legal obligations and business requirements:

- Consider incorporating a contractual right to review the vendor's annual security test results, business continuity and document management plan, and records management policies.
- Closely scrutinized indemnification and limitation of liability clauses to ensure risk is appropriately shared between vendor and business.

Before signing a contract renewal or extension, evaluate the course of the vendor relationship. Poor vendor performance can be indicative of data-security risk:

- Did the vendor's sales team over-promise and under-deliver?
- Do the service-level guarantees fall short?
- Was a risk mitigation identified that should be part of the agreement but the vendor does not want to put it in writing?
- Does the vendor fail to timely and accurately respond to inquiries about business-related issues and events?

These are all warning signs that the vendor may not be appropriately scaled to handle a particular project and that the vendor's data-security practices may be lacking.

Dig Deeper on Audit Results

Requesting that vendors provide the results of their latest information-security audit is an excellent entry point. Once results are provided, note the scope of the audit:

- A limited review of system access via Microsoft's Active Directory, for example, will not uncover security failures in the call center.
- A review of call center security procedures may neglect to highlight security failures in the vendor's enterprise cloud architecture.

Understanding where participant data is stored, where it is transferred when acted on by the business, whether it is encrypted when stored and transferred, when and how it is accessed and by whom is critical to understanding whether audit results are reliable.

In addition to scope, note the date and frequency of the vendor's audit process. It is recommended that audits be performed at least annually and as part of the remediation process following a breach.

Technology and regulatory requirements surrounding cybersecurity are rapidly evolving, and regular audits will help assure that a vendor is alerted to evolving security controls and legal requirements.

During the COVID-19 pandemic, many employees began working from home. For retirement plan vendors with remote employees, a cybersecurity audit performed post-pandemic should assess remote- work controls, including system access points such as VPN security and other web access points of entry.

More frequent security monitoring may be warranted for higher risk, critical functions and highly sensitive data. As attack methods and environmental changes develop rapidly, annual audits could lag in their assessment of the real security posture of a vendor.

Consider whether more frequent security assurances are needed, such as monthly or quarterly confirmation that risk assessments are still current and information is still secure.

Use a Vendor Security Questionnaire

Requiring vendors complete a security questionnaire can be a powerful tool for assessing a vendor's cybersecurity practices. A comprehensive questionnaire will do the following:

- Pinpoint risk areas and identify whether a vendor has implemented appropriate technical, process, and access controls to protect participant information.

- Provide a window into the architecture of a vendor's systems, which will help assess the appropriateness of the scope of vendor audits, and whether it has appropriate business-continuity plans.

A security questionnaire can be a critical tool for risk management and gaining comfort that the vendor is knowledgeable about the laws and regulations that govern confidential retirement plan information. It can also inform specific contractual provisions needed to ensure ongoing compliance with cybersecurity and information standards and practices.

Vendors should complete the security questionnaire annually, prior to or when submitting their annual information-security audit results.

Document, Document, Document

When the inevitable happens—a vendor data breach exposes a retirement plan participant's confidential data—scrutiny could follow. A business's vendor selection and management process and documentation might be dissected by regulatory authorities or through civil litigation.

Retirement plan sponsors are bound by fiduciary duties regarding vendor selection, including the duty of prudence. Take care to document the selection process, including the cybersecurity evaluation and criteria, and ongoing efforts to monitor cybersecurity compliance of existing vendors.

Demonstrating compliance with the DOL's best practice guidance will be a powerful defense against claims of imprudent vendor selection.

About the Author: Attorney Anton Janik, JD, LLM, CIPP/US, CIPP/E is an experienced trial attorney with a specialized practice in complex litigation, tax controversies and information security and privacy. Contact: ajanik@mwlaw.com.

This article was originally published online by the Society for Human Resource Management (SHRM) and is republished with written permission.