Professional Perspective

Surviving a DOL Cybersecurity Audit – A Cybersecurity Preparedness Checklist for Plan Fiduciaries

Elliot D. Raff and Harold J. Ashner, Keightley & Ashner LLP

Bloomberg Law

Surviving a DOL Cybersecurity Audit – A Cybersecurity Preparedness Checklist for Plan Fiduciaries

Contributed by Elliot D. Raff and Harold J. Ashner, Keightley & Ashner LLP

As stated by the U.S. Government Accountability Office (GAO) in its February 2021 report, the "sharing and storing of [information used to administer a defined contribution retirement plan] can lead to significant cybersecurity risks for plan sponsors and their service providers, as well as plan participants." See DEFINED CONTRIBUTION PLANS, Federal Guidance Could Help Mitigate Cybersecurity Risks in 401(k) and Other Retirement Plans (GAO-21-25). Following this GAO study, the U.S. Department of Labor, Employee Benefit Security Administration ("DOL") issued informal guidance concerning cybersecurity risks for employee benefit plan service providers, fiduciaries, and participants.

Just two months later, the DOL added cybersecurity to the list of topics it examines in *routine* plan investigations and began asking for a lengthy and detailed set of documents. Included in the DOL's request is an extensive list of documents relating to "any" cybersecurity programs that apply to the data of the plan -- thus encompassing not only programs of plan service providers, such as recordkeepers, but also programs of the employer and of other entities involved in plan operations, such as payroll service providers. Also included was another extensive list of documents relating to ongoing fiduciary review of service provider cybersecurity practices.

Whatever a particular fiduciary's degree of involvement with cybersecurity may be, the DOL's enforcement initiative should prompt the fiduciary to get ready for scrutiny of their own cybersecurity preparedness and oversight of the preparedness of their defined contribution retirement plan ("DC Plan") service providers, for example, 401(k) plan recordkeeper and institutional trustee.

Some Key Definitions

For the purposes of this article, there are a few technical terms that fiduciaries need to understand (unless otherwise noted, these definitions are taken from the GAO report referenced above):

- *Account Takeover* occurs when a threat actor gains access to the account and fraudulently transfers assets out of the account, for example, by first gaining online access to a 401(k) plan account, changing banking information, and then obtaining withdrawals diverted to their own bank account.

- *Personally identifying information* or "*PII*" is any information that can be used to distinguish or trace an individual's identity, such as name, date and place of birth, or Social Security number; and other types of personal information that can be linked to an individual, such as medical, educational, financial, and employment information.

- *Plan asset data* is sensitive information that is associated with a participant's retirement assets, such as their retirement account number and bank account information.

- *Threat actor* - The instigators of risks with the capability to do harm. *See* NISTIR 8286, Appendix B, p. 63.

Why This Is a Serious Problem to Which Fiduciaries Should Pay Attention

There are several structural factors that make cybersecurity with respect to DC Plans generally, and account takeover specifically, issues of critical importance:

- DC Plans, such as 401(k) plans, are ubiquitous – the GAO study reported that, as of 2018, 106 million people participated in private sector DC Plans, which held assets of nearly $6.3 trillion.

- There is no comprehensive federal guarantee of lost DC Plan benefits. Thus, if a 401(k) plan account is stolen through an account takeover, there is no federal program to restore the account balance or otherwise make the victim whole.

- The administration of a 401(k) plan entails a constant flow of PII among the employer, payroll service provider, recordkeeper, and trustee, each of which is also storing this PII for long periods of time. Thus, service providers face constant attacks to obtain PII and attempts at account takeover.

- As PII can be purchased in bulk on the dark-web and log-in attempts can be automated, it is unfortunately all too easy for a threat actor to take over an account.

- Anecdotal evidence indicates that many participants do not read plan communications, and therefore a transaction confirmation in many cases is not read and the transaction goes unnoticed by the participant. Further, unlike debit and credit cards with respect to which banks have developed real-time anti-fraud monitoring and alerts, *e.g.*, a text message inquiring about a recent purchase, institutions generally have not created a similar system with respect to DC Plans.

DOL Guidance

On April 14, 2021, the DOL issued informal guidance concerning cybersecurity and ERISA-covered employee benefits plans, with a focus on DC Plans generally, and 401(k) plans specifically. The DOL's guidance consists of:

- Cybersecurity Program Best Practices ("Best Practices"): This is primarily for use by plan recordkeepers and other service providers who are responsible for plan-related IT systems and/or data.

- Tips for Hiring a Service Provider with Strong Cybersecurity Practices ("Hiring Tips"): This is intended to help plan fiduciaries satisfy their fiduciaries duties with respect to selecting and monitoring plan service providers.

- Online Security Tips ("Participant Tips"): These are tips for plan participants on how to protect their PII.

In its Best Practices, the DOL made clear its position that "*[r]esponsible plan fiduciaries have an obligation to ensure proper mitigation of cybersecurity risks*" (emphasis added). This means that a prudent service provider selection process must incorporate consideration of cybersecurity procedures and that ongoing review of service provider performance (to ensure that a selection remains prudent) must include review of the service provider's cybersecurity procedures. Indirectly, this also means that service provider agreements should incorporate provisions reflecting (to an appropriate degree) the agreed upon cybersecurity procedures and the reporting and disclosure needed to review periodically the service provider's compliance with its procedures.

DOL Enforcement Initiative

As indicated above, the DOL recently added cybersecurity to its plan investigation issues list and started asking for extensive cybersecurity related documentation. The DOL's Information and Document Requests are very broad, for example, requesting:

> "all documents relating to any cybersecurity or information security programs that apply to the data of [the Plan], whether those programs are applied by the sponsor of the Plan or by any service provider of the Plan." (Emphasis added).

The DOL then lists a large number of items included in this broad request, starting with "All policies, procedures, policies or guidelines relating to:"

- Data governance, classification, and disposal;

- The implementation of access controls and identity management, including any use of multi-factor authentication;

- The processes for business continuity, disaster recovery, and incident response;

- The assessment of security risks;

- Data privacy;

- Management of vendors and third party service providers, including notification protocols for cybersecurity events and the use of data for any purpose other than the direct performance of their duties;

- Cybersecurity awareness training; and
- Encryption to protect all sensitive information transmitted, stored, or in transit.

Also included in the broad DOL request are all of the following:

- All documents and communications relating to any past security incidents;
- Security risk assessment reports;
- Security control audit reports, audit files, penetration test reports and supporting documents, and any other third-party cybersecurity analyses;
- Documents describing any secure system development life cycle (SDLC) program, including penetration testing, code review, and architecture analysis; and
- Documents describing security technical controls, including firewalls, antivirus software, and data backup.

Finally, the DOL seeks, as yet another part of its broad request, all documents and communications:

- Describing security reviews and independent security assessments of the assets or data of the plan stored in a cloud or managed by service providers;
- From service providers relating to their cybersecurity capabilities and procedures;
- From service providers regarding policies and procedures for collecting, storing, archiving, deleting, anonymizing, warehousing, and sharing data; and
- Describing the permitted uses of data by the sponsor of the plan or by any service providers of the plan, including, but not limited to, all uses of data for the direct or indirect purpose of cross-selling or marketing products and services.

These are obviously massive requests, and even fiduciaries who engaged in rigorous due diligence when selecting a service provider, when negotiating or renegotiating service agreements, and who have engaged in prudent ongoing oversight may have difficulty producing the full extent of the requested documents. However, since the DOL requests largely trace back to the Best Practices and Hiring Tips, which provide broad and specific guidance, the breadth and specificity of the requests are not surprising.

Fiduciary Action Plan

Whether a fiduciary has been highly engaged with cybersecurity or not, the following outlines a fiduciary action plan:

(a) Get Informed. Fiduciaries should get informed about cybersecurity governance, *i.e.*, ensuring high-level oversight responsibility for cybersecurity, generally, and more specifically about cybersecurity threats to plans and plan benefits. A good place to start is the GAO Report referenced above.

(b) Get Expert Support, if Needed. If fiduciaries lack the expertise to assess cybersecurity procedures, they should get support from an expert, who may be an in-house resource, such as someone from the employer's data security staff, or an outside consultant.

(c) Data Flow & Storage. Fiduciaries should identify all the parties involved in plan operations and determine who transmits what PII and/or plan asset data to whom, and who stores what data.

(d) Assess Fiduciary Conduct to Date. For better or worse, assessing fiduciary conduct to date is a critical first big step. Section 5, below, contains a Cybersecurity Preparedness Checklist for Plan Fiduciaries to assist with this process.

(e) Develop and Implement a Service Provider Cybersecurity Strategy. Completing the Cybersecurity Preparedness Checklist for Plan Fiduciaries should help identify gaps in documentation and/or weaknesses in the fiduciary process in relation to cybersecurity and service providers. Review of the results of an initial

assessment based on the checklist should form the basis for a strategy to close the gaps and to improve ongoing fiduciary oversight.

Document the Activities. The best way to demonstrate prudent conduct is through contemporaneous documentation in the form of reports to fiduciary committees and meeting minutes reflecting discussion of and decisions concerning the key issues.

Cybersecurity Preparedness Checklist for Plan Fiduciaries

Fiduciaries should complete the Cybersecurity Preparedness Checklist for Plan Fiduciaries 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.

Conclusion

401(k) plans face significant cybersecurity risks for which there is no federal safety net. Service providers are very much on the front line, but plan fiduciaries need to treat cybersecurity with the same high degree of diligence that they exercise in relation to investment decision-making and all other plan administrative matters. The key to mitigating risk is conducting a self-assessment using the Cybersecurity Preparedness Checklist for Plan Fiduciaries and building a strategy around the results of that assessment.