

Employee Benefit Plan Review

Ask the Experts

BY MARJORIE M. GLOVER, DAVID GALLAI, AND RACHEL M. KURTH

DOL CYBERSECURITY GUIDANCE FOR ERISA RETIREMENT PLANS

Q My company sponsors a 401(k) plan, and I heard that there is some recent guidance about cybersecurity that retirement plan sponsors should be aware of. Is that true, and what is the guidance?

A Yes, that is correct, the U.S. Department of Labor (“DOL”) recently published new guidance for plan sponsors, plan fiduciaries, recordkeepers and plan participants on best practices for maintaining cybersecurity, including tips on how to protect retirement benefits. This is the first time that the DOL’s Employee Benefits Security Administration (“EBSA”) has issued guidance on cybersecurity. The new EBSA guidance consists of three separate publications:

- (1) *Cybersecurity Program Best Practices*, which provides guidance to plan fiduciaries and recordkeepers on their responsibilities managing cybersecurity risks. This guidance is available at: <https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/best-practices.pdf>.
- (2) *Tips for Hiring a Service Provider with Strong Cybersecurity Practices*, which provides guidance to plan sponsors and fiduciaries on prudently selecting a service provider with strong cybersecurity practices and monitoring their activities, consistent

with ERISA’s requirements. This guidance is available at: <https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/tips-for-hiring-a-service-provider-with-strong-security-practices.pdf>.

- (3) *Online Security Tips*, which offers plan participants and beneficiaries who check their retirement accounts online basic guidance to reduce the risk of fraud and loss. This guidance is available at: <https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/online-security-tips.pdf>.

EBSA’s guidance on *Cybersecurity Program Best Practices* states that plans’ service providers should:

- Have a formal, well documented cybersecurity program;
- Conduct prudent annual risk assessments;
- Have a reliable annual third party audit of security controls;
- Clearly define and assign information security roles and responsibilities;
- Have strong access control procedures;
- Ensure that any assets or data stored in a cloud or managed by a third party service provider are subject to appropriate security reviews and independent security assessments;
- Conduct periodic cybersecurity awareness training;

■ Ask the Experts

- Implement and manage a secure system development life cycle program;
- Have an effective business resiliency program addressing business continuity, disaster recovery, and incident response;
- Encrypt sensitive data, stored and in transit;
- Implement strong technical controls in accordance with best security practices; and
- Appropriately respond to any past cybersecurity incidents.

EBSA's guidance on *Tips for Hiring a Service Provider with Strong Cybersecurity Practices* provides tips to help business owners and fiduciaries meet their responsibilities under ERISA to prudently select and monitor service providers, including:

- Asking about the service provider's information security standards, practices and policies and audit results, and comparing them to the industry standards adopted by other financial institutions;
- Asking the service provider how it validates its practices and what levels of security standards it has met and implemented;
- Evaluating the service provider's track record in the industry, including public information regarding information security incidents, litigation, and legal proceedings related to the vendor's services;
- Asking whether the service provider has experienced past security breaches, what happened, and how the service provider responded;
- Finding out if the service provider has any insurance policies that would cover losses caused by cybersecurity and identity theft breaches; and
- When contracting with a service provider, ensuring that the contract requires ongoing compliance with cybersecurity and


information security standards (and does not limit the service provider's responsibility for IT security breaches), and trying to include additional contract terms that would enhance cybersecurity protection for the retirement plan and its participants.

EBSA's security guidance for participants and beneficiaries urges them to take steps to secure their online retirement accounts, such as:

- Registering, setting up, and routinely monitoring their online accounts;
- Using strong and unique passwords;
- Using multi-factor authentication;
- Keeping personal contact information current;
- Closing or deleting unused accounts;
- Avoiding free WiFi;
- Watching out for phishing attacks;
- Using antivirus software and keeping apps and software current; and
- Knowing how to report identity theft and cybersecurity incidents.

We recommend that you familiarize yourself with the DOL's new cybersecurity guidance and follow their recommendations when developing or evaluating the cybersecurity practices of your retirement plan's service providers and entering into contracts with such service providers.

TUITION REIMBURSEMENT PROGRAM

 My company sponsors a tuition reimbursement program. We are thinking of expanding it to provide for repayment of student loans. Do we need to set up a separate plan or may we amend our existing program? Are we required to make the student loan repayment feature available to all our employees or can we offer it only to

employees in certain locations or job classifications?

A The Coronavirus Aid, Relief and Economic Security ("CARES") Act, passed in March 2020, permitted employers to provide up to \$5,250 in student loan repayments or tuition assistance from March 27, 2020 through December 31, 2020. In December 2020, the Consolidated Appropriations Act extended the student loan repayment provision through the end of 2025.

This provision allows employers to provide pay student loans of up to \$5,250. The total amount of the student loan payment plus any tuition assistance may not exceed \$5,250 per year.

It is not necessary to establish a new tuition reimbursement program. The student loan repayment feature may be added to an existing program.

The new student loan repayment provisions must meet the requirements for educational assistance programs under Internal Revenue Code ("IRC") Section 127. Pursuant to IRC Section 127, benefits must be provided benefit employees who qualify under a classification that does not discriminate in favor of highly compensated employees (\$130,000 for 2021) or their dependents.

For this purpose, employees covered under a collective bargaining unit may be excluded if there is evidence that the educational assistance benefits were the subject of good faith bargaining. In addition, not more than five percent of the amounts paid or incurred by the employer for educational assistance during the year may be provided to a class of individuals who are shareholders or owners (or their spouses or dependents), each of whom (on any day during the year) owns more than five percent of the stock or capital or profits interest in the employer.

It may be possible to structure your company's educational

assistance program to provide benefits to employees at certain locations or to certain classes, if the non-discrimination and five percent owner limits are met. You did not mention whether your company has collectively bargained employees. If your company does have collectively bargained employees, it may be permissible to limit benefits to non-collectively bargained employees if the benefits were the subject of good faith bargaining.

In either case, if you do choose to offer the benefit, it is important to amend your plan document and to communicate the change in benefits to employees. 🌐

Marjorie M. Glover, a partner in the New York City office of Norton Rose Fulbright US LLP, focuses her practice on executive compensation and employee benefits law, corporate governance and risk oversight and employment law.

David Gallai, who also is a partner in the firm's New York City office, practices in the areas of employment counseling, executive compensation, and employee benefits. Rachel M. Kurth is a senior counsel at the firm. They can be reached at marjorie.glover@nortonrosefulbright.com, david.gallai@nortonrosefulbright.com, and rachel.kurth@nortonrosefulbright.com, respectively.

Copyright © 2021 CCH Incorporated. All Rights Reserved.
Reprinted from *Employee Benefit Plan Review*, June 2021, Volume 75,
Number 5, pages 4–5, with permission from Wolters Kluwer, New York, NY,
1-800-638-8437, www.WoltersKluwerLR.com

