masuda funai

News & Types: Employment, Labor & Benefits Update

Protecting Employee Retirement Savings from Cyber Criminals

6/23/2021

By: Frank J. Del Barto

Practices: Employment, Labor & Benefits

Companies that sponsor 401(k) plans have a fiduciary obligation to protect the individual retirement accounts of their employees from cyber theft. Currently, there are approximately 106 million defined contribution plans in the United States, which hold almost $6.3 trillion in employee retirement savings. For many employees, their individual 401(k) account represents their largest asset and their sole retirement savings vehicle. Unfortunately, over the last couple of years, cyber theft has become an increasing risk for companies that sponsor 401(k) plans. In one case, a former employee had $245,000 withdrawn from her individual 401(k) account by cyber criminals. In another case, a law firm partner had $400,000 withdrawn from his individual 401(k) account by cyber criminals.

Recognizing cyber criminals pose a real threat to retirement plans, the U.S Department of Labor ("DOL") recently issued cyber security best practice guidance for companies that sponsor 401(k) plans, plan fiduciaries, record-keepers, and employees who participate in 401(k) plans. This is the first time the DOL has issued cybersecurity guidance. The DOL's guidance comes in three forms: (1) Tips for Hiring a Service Provider, which is intended to help companies that sponsor a 401(k) plan in selecting a service provider with strong cybersecurity practices and procedures; (2) Cybersecurity Program Best Practices, which provide twelve broad categories of best practice guidelines to help mitigate cyber security risks, and (3) Online Security Tips, which are intended to assist individual employees in reducing the risks of fraud and loss to the their individual 401(k) retirement savings account.

In accordance with ERISA section 404, a plan fiduciary must discharge his/her duties with respect to the 401(k) plan solely in the interest of employees and plan beneficiaries and for the exclusive purpose of providing them retirement benefits. As a result, a partial or total loss of an employee's 401(k) account balance due to cyber theft may be considered a breach of fiduciary duty, which exposes the fiduciary to personal liability and the requirement to make the plan whole. In the examples noted above, the thefts of the employee's retirement savings have resulted in litigation against the employee's company and other entities who were involved in plan administration. To avoid the loss of employee account balances due to cyber theft, companies must review and implement the DOL guidance to reduce the risk of cyber theft. Because cyber criminals are becoming increasingly more sophisticated, cybersecurity will be an ongoing responsibility and obligation and not a one-time review for companies that sponsor 401(k) plans.