AUTOMATIC ENROLLMENT IS ON THE RISE

WITH THE FUTURE OF SOCIAL SECURITY IN QUESTION, IT IS BECOMING EVER INCREASINGLY IMPORTANT FOR WORKERS TO SELF-PREPARE FOR POST-RETIREMENT LIVING. Studies show that approximately one out of every three eligible workers choose NOT to participate in their employer-sponsored 401(k) plan. Offering automatic enrollment in your 401(k) plan is a way for you, as Plan Sponsor, to help lend a hand to employees that are not fully aware of the significance of having a post-retirement source of revenue.

Plans with an automatic enrollment feature nearly doubled over the past decade according to the Plan Sponsor Council of America's (PSCA) 60th Annual Survey of Profit Sharing and 401(k) Plans. PSCA, part of the American Retirement Association, found that 59.7 percent of plans had an automatic enrollment feature in 2016 compared to 35.6 percent in 2007. Having an automatic enrollment provision can also help allow Highly Compensated Employees (HCE's) contribute more to the plan by either boosting the participation rate of Non-Highly Compensated Employees (NHCE's) or by satisfying the Safe Harbor requirements which exempt the plan from certain nondiscrimination testing.

Your current plan document gives you the option to choose different levels of automatic enrollment, described in the following paragraphs.

AUTOMATIC CONTRIBUTION ARRANGEMENT

The Automatic Contribution Arrangement (ACA) is the most basic of the automatic enrollment options and has existed since the late 1990's. A 401(k) plan with an ACA provides for increased participation by stating that eligible employees will be automatically enrolled in the plan unless they elect otherwise. A beginning "default" withholding percentage or dollar amount is chosen by you as the Plan Sponsor. Employees have the right to choose not to have salary deferred, or to elect a percentage or dollar amount that is different from the default withholding.

If the ACA provision is newly added to the plan, you as the Plan Sponsor may elect to apply the automatic enrollment to existing participants or apply it solely to new employees moving forward. If your plan allows for Roth deferrals, the default withholding may be traditional pre-tax 401(k) or Roth-based. You even have the option of escalating the initial automatic deferral amount annually for employees, thus increasing their savings every year of employment.

DID YOU KNOW?

More than half of plans with automatic enrollment are only set up for new hires.

401k Specialist Magazine, June 2018

In the event that a discretionary company match is offered, automatically-enrolled employees' contributions are matched just as they normally would be for employees that voluntarily participate. Any discretionary contributions follow your plan's regular vesting schedule.

ELIGIBLE AUTOMATIC CONTRIBUTION ARRANGEMENT

The Eligible Automatic Contribution Arrangement (EACA) builds on the basic ACA. All aspects mentioned above also apply to EACA's, with two primary additions:

1. The plan has the option to choose to allow permissible withdrawals for employees that were initially automatically enrolled, but then elected not to participate in the plan.

2. A window of 30-90 days may be chosen within the date of the first automatic deferral to allow participants who were automatically enrolled to "opt-out" and withdraw any money that was already withheld from their pay. Any associated company match would, in turn, be forfeited.

If your EACA plan covers all employees, the deadline to complete your ADP/ACP nondiscrimination testing and withdraw any necessary testing failure refunds without a penalty is six months following the close of the Plan year, rather than two and a half months following the close of a plan year for a non-EACA plan.

QUALIFIED AUTOMATIC CONTRIBUTION ARRANGEMENT

A Qualified Automatic Contribution Arrangement (QACA) combines automatic enrollment provisions with the IRS' Safe Harbor provisions. Thus, QACA plans increase participation among employees while also making the plan exempt from certain nondiscrimination testing and allow HCE's to maximize their annual 401(k) contributions. QACA provisions require a minimum of 3% automatic enrollment; however, certain annual escalations may be necessary such that by year five, an automatically enrolled employee must have at least a 6% contribution rate. You may opt to begin year one with 6% as the automatic enrollment percentage to avoid the required escalations, but in no event can the automatic withholding exceed 10% of annual compensation.

Unlike the other automatic enrollment arrangements, QACA plans have a required employer contribution. An employer must make at least a 100% matching contribution of salary deferrals up to the first 1% of compensation, plus a 50% matching contribution on the next 5% of compensation deferred, or a non-elective contribution equal to 3% of compensation to all eligible participants. Either of these contributions must be fully vested by the time an employee has completed two years of service.

QUALIFIED DEFAULT INVESTMENT ALTERNATIVE

All automatic enrollment options may elect a Qualified Default Investment Alternative (QDIA). The default fund is utilized when an employee does not make their own investment election but is entitled to a contribution in the plan – whether being their own salary deferrals, company funded contributions, and/or reallocated forfeitures. A QDIA requires an annual notice be provided to your employees, summarizing the plan's QDIA selection.

The purpose of the QDIA is to minimize the risk of large losses and at the same time provide long-term growth. Choosing a QDIA offers liability relief to an extent for plan fiduciaries. Your investment advisor may be able to provide you with more details regarding what funds constitute a QDIA. While not required by law for an ACA, EACA, or QACA, most automatic enrollment plans do elect a QDIA for administrative convenience.

If you are interested, please contact McCloud & Associates, Inc. to see how automatic features can help boost the retirement savings of your employees.

PROTECT YOUR 401(K)

THOUGH SOME EMPLOYERS MAY NOT THINK SO, THE TRUTH IS THAT IN TODAY'S WORLD 401(K) PLANS ARE SUBJECT TO FRAUDULENT ACTIVITY AND THAT THE OFTEN-OVERLOOKED RETIREMENT PLAN CAN BE THE PERFECT PLACE FOR IT TO OCCUR. For example, in late 2017, several news outlets reported a scheme targeting individual 401(k) accounts. The U.S. Attorney's office in Colorado had filed a lawsuit to recover up to $2 million in losses due to fraudulent distributions from retirement plan accounts. The lawsuit, filed December 4th, 2017 in federal court, sought to seize up to $342,335 in assets from five individuals that deposited funds from the alleged scheme. Multiple banks, including JP Morgan Chase Bank, Bank of America, PNC Bank, and Wells Fargo, received the fraudulent transactions. According to the suit, the FBI's Denver Division was contacted in November 2016 by Great-West Financials' VP of Internal Audit regarding allegations of fraudulent transfers from clients' 401(k) accounts by JP Morgan. At that time, Great-West Financial had 20 participants affected with a loss of at least $1 million and a potential loss in excess of $2 million.

As in many 401(k) plans, participant victims of the fraud established an account online with the plan's recordkeeper (in this case Great-West). Great-West maintains a call center to assist with questions when contacted by a plan participant, utilizing a four-part authentication process that employs biographical identifiers set up by the plan participant. Using this biographical information (e.g. name, Social Security numbers, or date of birth) obtained through phishing scams and password hacking, the scammers were able to provide accurate information to change the online profile and ultimately affect a distribution. According to the suit, Great-West observed that unauthorized individual(s) had been fraudulently using this process to obtain access to funds held in retirement accounts. Upon obtaining access, the funds were able to be transferred from those retirement accounts to other bank accounts without the knowledge or consent of the actual participant. The FBI indicated that Great-West wasn't the only recordkeeper that was targeted by fraud schemes. In the end, Great-West reimbursed all funds to the participant's account.

Please note, in this instance, neither the TPA nor Great-West had experienced a data breach. The participant's personally identifiable information (PII) was obtained by other means prior

Upcoming Compliance Deadlines for Calendar-Year Plans (12 / 31)

15th — May 2019

Deadline for participant-directed plans to supply participants with the quarterly benefit/disclosure statement including a statement of plan fees and expenses charged to individual plan accounts during the first quarter of this year.

1st — July 2019

EACA ADP/ACP Corrective Testing – ADP/ACP refunds are due to highly compensated employees (HCEs) to avoid a 10% excise tax on the employer for plans that have elected to participate in an Eligible Automatic Enrollment Arrangement. Note: Deadline is normally June 30, which this year falls on a Sunday.

15th

Defined Benefit Contributions – Deadline for Defined Benefit Plans to make the second quarter contribution.

29th

Summary of Material Modifications (SMM) - A SMM is due to participants no later than 210 days after the end of the plan year if a plan change or amendment was adopted in that year.

31st

Due date for calendar-year plans for the filing of **Form 5500** (Annual Return Report of Employee Benefit Plan), **Form 5558** (Application for Extension of Time to File Certain Employee Plan Returns), **Form 5330** (Return of Excise Taxes Related to Employee Benefit Plans), and **Form 8955-SSA** (Annual Registration Statement Identifying Separated Participants With Deferred Vested Benefits).

McCloud & Associates, Inc.

QUALIFIED PLAN CONSULTING AND ADMINISTRATION

SPECIALIZING IN PLAN DESIGN FOR:

- 401(k) Plans
- Safe Harbor 401(k) Plans
- Profit Sharing Plans
- Cash Balance Plans
- Traditional Defined Benefit Plans

CONTACT US:

McCloud & Associates, Inc.
200 W. Mill Street
Liberty, MO 64068
816.792.3838
info@mccloudandassociatesinc.com
www.mccloudandassociatesinc.com

to contacting Great-West or submitting the distribution request. It appears that the PII was obtained through scams aimed at the participant. This being the case, what can you do to help mitigate distribution fraud?

• EDUCATE YOUR PARTICIPANTS on password management. Many times, the retirement plan account password is the same, or very similar, to another password in an account that may have been breached. Changing passwords and using stronger, randomly-generated passwords goes a long way towards protecting PII.

• REVIEW YOUR ACCOUNT transactions. Online access that is available 24/7/365 has taken the scrutiny from quarterly or annual statements. Reviewing your account on a frequent basis can help identify fraudulent activity quickly.

• DON'T USE SECURITY QUESTIONS in a participant's profile the hacker may potentially be able to find the answers to from information which can be found publicly, such as on social media.

• ASK FOR VERIFICATION of distributions and loans if the recordkeeper allows for it. It might seem to be an excessive burden to approve individual transactions but checking with an employee by cell phone or protected communication channels will prevent a lot of problems down the road. Remember, if the participant's email was the source of the hacked information, the hacker could still be accessing email accounts undetected.

• ESTABLISH A SYSTEM of checks and balances within your own human resources and accounting departments. Fraud can occur in many ways, and hacking seems to be the most prevalent today. Internal personnel have the power to request and direct retirement distributions for the plan's recordkeeper.

It's good practice to review your retirement plan's transactions each month like you would your company bank account or credit card accounts. If you see any questionable transactions, please contact McCloud & Associates, Inc. immediately.

DID YOU KNOW?

On average, it takes 196 days for a company to identify a data breach.

Norton Security, 2019