TRUCKER ✦ HUSS

BENEFITS REPORT

SPECIALIZED TALENT & EXPERTISE TO SOLVE THE MOST COMPLEX OR STRAIGHTFORWARD CLIENT CHALLENGES.

With more than 25 attorneys practicing solely in employee benefits law, Trucker Huss is the largest employee benefits specialty law firm on the West Coast. Our in-depth knowledge and breadth of experience on all issues confronting benefit plans, plan sponsors and plan fiduciaries translates into real-world, practical solutions for our clients.

A DIVERSE CLIENT BASE. We represent some of the country's largest companies and union sponsored and Taft-Hartley trust funds. We also represent mid-sized and smaller employers, benefits consultants and other service providers, including law firms, accountants and insurance brokers.

PERSONAL ATTENTION AND SERVICE, AND A COLLABORATIVE APPROACH. Since its founding in 1980, Trucker Huss has built its reputation on providing accurate, responsive and personal service. The Firm has grown in part through referrals from our many satisfied clients, including other law firms with which we often partner on a strategic basis to solve client challenges.

NATIONALLY-RECOGNIZED. Our attorneys serve as officers and governing board members to the country's premier employee benefits industry associations, and routinely write for their publications and speak at their conferences.

TRUCKER ✦ HUSS
A PROFESSIONAL CORPORATION
ERISA AND EMPLOYEE BENEFITS ATTORNEYS

One Embarcadero Center, 12th Floor
San Francisco, California 94111-3617
Tel: (415) 788-3111
Fax: (415) 421-2017
Email: info@truckerhuss.com

633 West 5th Street, 26th Floor
Los Angeles, California 90071-2053
Tel: (213) 537-1016
Fax: (213) 537-1020

www.truckerhuss.com

California to Move Forward with Auto-IRA Despite Loss of ERISA Safe Harbor

T. KATURI KAYE

On May 18, 2017, California State Treasurer John Chiang and Senate President Pro Tempore Kevin de León (D-Los Angeles) issued a press statement announcing that California remains on track to implement the California Secure Choice Retirement Savings Program ("Secure Choice" or the "Program"), a state-sponsored program requiring employers that do not offer workplace savings arrangements to establish an automatic payroll-deduction program to facilitate individual retirement account ("IRA") contributions by participating employees. (These programs are also referred to in this article as "auto-IRAs" or "auto-IRA programs.") California's announcement came on the heels of Congress passing joint resolutions (which were ultimately signed by President Trump) to nullify prior final regulations issued by the Department of Labor ("DOL") making auto-IRAs exempt from coverage under the Employee Retirement Income Security Act of 1974 ("ERISA"). Despite the reversal, California intends to fully implement Secure Choice, which is described on the California State Treasurer's Secure Choice website as being "*the most ambitious push to expand retirement security since the passage of Social Security in the 1930s*." This article addresses the background on auto-IRAs, the history of Secure Choice, the impact of the auto-IRA safe harbor and its reversal, and the effect on California employers.

IN THIS ISSUE...

Trucker ✦ Huss is proud to be a sponsor of the 2017 Western Benefits Conference in Anaheim, CA, to be held July 9 – 12, at the Hilton Anaheim. This is certain to be a premier educational and networking opportunity for retirement and health & welfare benefits professionals, and our attorneys are actively involved as committee members and presenters. Early registration ends June 16. We look forward to seeing you in Anaheim!

Background on Auto-IRAs

In recent years, prompted by the concern that millions of U.S. workers do not have access to workplace retirement savings programs, several states have enacted legislation establishing state-sponsored auto-IRA programs. In order to allow private-sector employees to contribute salary withholdings to IRAs, these programs generally require employers that do not offer workplace retirement savings programs to automatically deduct a specified amount of wages from employees' paychecks and remit those amounts to state-administered IRAs established for participating employees. These auto-IRA programs are intended to extend access to, and coverage under, the private retirement system, resulting in overall improvement in retirement security for countless U.S. workers.

To date, California, Connecticut, Illinois, Maryland, Oregon and Vermont are among the several states that have adopted legislation enacting state-sponsored auto-IRAs.

The California Secure Choice Program

On February 23, 2012, the California legislature enacted Senate Bill 1234, establishing the California Secure Choice Retirement Savings Trust Act (the "Act"). The Act created the California Secure Choice Retirement Savings Trust ("Trust"), to be administered by the California Secure Choice Retirement Savings Investment Board ("Board"). Under the Act, the Board was instructed to design and establish Secure Choice for the more than six million California workers who lack access to retirement savings plans through their private-sector employers. The Act required that a feasibility study be conducted to determine the level of interest in the Program and whether it would be financially viable without the ongoing use of taxpayer funds.

On September 29, 2016, California Governor Brown approved amendments to the Act, which took into account the results of years of studies and expressed legislative approval of Secure Choice's implementation on January 1, 2017.

Although Secure Choice was scheduled to be implemented on January 1, 2017, an employer alert on the California State Treasurer's Secure Choice website recently provided that the Program will not go into effect for at least two years, with 2019 likely being the earliest year large employers that do not offer a retirement plan to their employees will be required to provide access to the Program. Once implemented, however, Secure Choice will require private-sector employers in California with five or more employees that do not already provide a retirement plan to either begin offering a retirement plan or provide their employees with access to the Program. Specifically:

- private-sector employers with more than 100 employees will be required to offer a retirement

plan within 12 months after the Program becomes open for enrollment;

- private-employers with more than 50 employees will be required to offer a retirement plan within 24 months after the Program becomes open for enrollment; and
- private-employers with more than five employees will be required to offer a retirement plan within 36 months after the Program becomes open for enrollment.

In addition, employers will be required to automatically enroll all eligible employees in Secure Choice, unless an employee expressly opts out of participation.

Secure Choice is also intended to be operated in a manner that would impose limited responsibilities on participating employers, other than performing general administrative duties, such as enabling employees to make automatic contributions from their paycheck into their auto-IRAs, transmitting payroll contributions to a third-party administrator to be determined by the Board, and providing state-developed informational materials about the Program to eligible employees.

Moreover, the Board has made clear that there will be limits on employer liability under Secure Choice. For example, employers will not have any liability for an employee's decision to participate in, or opt out of, the Program, nor will they have any liability for the investment decisions of participating employees. Furthermore, employers will not be considered fiduciaries of the Program. More importantly, employers will not be able to contribute to their employees' accounts, as such contributions may trigger ERISA-coverage.

Overall, the intent of the fully operational Program, as articulated by the Board and California legislature, is to provide for auto-IRAs without subjecting Secure Choice or participating employers to ERISA-coverage and related potential liability thereunder.

How ERISA-Coverage Can Extend to an Auto-IRA Program

To be an employee benefit plan covered by ERISA, a plan must be established or maintained by an employer or by an employee organization. Thus, if a plan or program is considered maintained by the employee, then it is not an employee pension benefit plan covered by Title I of ERISA. IRAs ordinarily are established by individuals without any employer involvement. As a result, IRAs generally are not subject to Title I of ERISA because they are not maintained by an employer.

Where an employer has a payroll deduction program that permits employees to contribute to IRAs, the DOL has previously ruled, under DOL Regulations Section 2510.3-2(d) and Interpretive Bulletin 99-1, that such IRAs are not subject to Title I of ERISA if certain conditions are satisfied, including the following:

(i) No contributions are made by the employer to the IRA (other than through payroll deduction, by which the employer simply transmits the contribution directly to the employee's IRA as a means of facilitating the employee's funding of the IRA);

(ii) Participation in the IRA is completely voluntary for employees;

(iii) The sole involvement of the employer is to permit the IRA-sponsor to publicize the program to employees, to collect contributions through payroll deductions, and to remit contributions to the IRAs; and

(iv) The employer receives no consideration in the form of cash or otherwise, other than reasonable compensation for services actually rendered in connection with payroll deductions.

Particularly relevant to the issue of ERISA-coverage is the "completely voluntary" requirement under (ii) above. The DOL has interpreted this requirement as precluding the use of an automatic enrollment feature. Accordingly, from the DOL's perspective, having an automatic payroll deduction IRA program would constitute the establishment of a plan for ERISA purposes.

Auto-IRA ERISA Safe Harbor – Issuance and Reversal

Considering the influx of states establishing legislation requiring private-sector employers to establish auto-IRAs and the rising concern of employers that the automatic enrollment provisions of these programs would subject

them to ERISA-coverage, the DOL issued final regulations that created a new safe harbor for auto-IRAs, which we previously reported on in our August 2016 Benefits Report. Under the final regulations, effective October 31, 2016, the DOL described the circumstances in which states could offer auto-IRAs without giving rise to the establishment of an employee benefit plan under ERISA. The DOL later expanded the safe harbor to cover political subdivisions, such as counties and cities, as described in our earlier newsletter. The objective of the new safe harbor was to reduce the risk of auto-IRA programs from being preempted by ERISA, if ever challenged.

In February of this year, however, the House of Representatives ("House") took action to nullify the DOL's auto-IRA safe harbor by passing two resolutions revoking the safe harbor rule for both states and political subdivisions. Then in May of this year, following the House's action, the Senate voted in favor of passing a joint resolution overturning the DOL's auto-IRA safe harbor. President Trump ultimately signed legislation on May 17, 2017 that overturned the DOL's auto-IRA safe harbor rule in its entirety. As a result, states and political subdivisions that choose to sponsor auto-IRA programs currently have no assurance from the DOL that such programs are exempt from ERISA-coverage.

California's Response

While the federal government has reversed the DOL's auto-IRA safe harbor rule, California has made it clear that such actions will not undo the work that has been done. In a press statement on the California State Treasurer's website, dated May 3, 2017, Treasurer Chiang said, "While I am deeply disappointed in this most recent example of the typical Beltway deal-making, which always seems to favor Wall Street bankers over Main Street workers, I am more resolute than ever to standing-up Secure Choice so that all Californians can have a dignified retirement."

Secure Choice is not intended go into effect until the program is fully operational, which may not be for at least another two years, as noted on the California State Treasurer's Secure Choice website. It will then be phased in over a three-year period. The goal is for the Program to begin operations sometime in 2018. That means employers with 100 or more employees that do not offer a retirement plan will be required to provide a retirement plan or access to Secure Choice in 2019. Employers with more than 50 employees will be mandated to participate within two years after the Program is open for enrollment, which is likely to be 2020, and within 36 months all employers with fewer than 50 employees will be required to participate. Therefore, the Program is anticipated to be fully rolled out in 2021.

California legislatures have indicated that although they intend to eliminate the reference to the DOL's auto-IRA safe harbor from the Act, the requirement that the Secure Choice program may not be an ERISA-regulated plan is expected to remain once the program is fully operational. During a press conference held on May 18, 2017, Treasurer Chiang stated that he has consulted with legislative leaders and legal counsel and is "*confident that California is on a strong legal footing in moving forward to make Secure Choice a reality*."

Final Notes

Although the non-ERISA status of auto-IRAs has not been challenged in court, the private retirement community will be watching for how the ERISA-exemption argument holds for states, such as California, that are pressing forward with these types of programs without the DOL's auto-IRA safe harbor. Furthermore, it will be noteworthy to see if the loss of the DOL's auto-IRA safe harbor will discourage more states from joining California. Interestingly enough, the problem of inadequate retirement savings and the consequences of insufficient retirement planning are becoming a significant economic burden on not just the states and political subdivisions, but the federal government as well. However, supporters of the DOL's auto-IRA safe harbor believe that the federal government, by revoking the safe harbor auto-IRA, has created an obstacle for private-sector workers by limiting opportunities to accumulate greater retirement savings.

We will continue to monitor the status of auto-IRAs and Secure Choice, and advise you of any significant developments.

JUNE 2017

Cybersecurity and ERISA: Fiduciary Obligations to Safeguard Plan Participants' Data

ARIEL GAKNOKI

There have been numerous instances of high-profile cybercrime cases over the past couple of years spurring lively discussions in the ERISA community about the potential threat this type of crime poses to plan assets and personal data of plan participants and beneficiaries. Except when there has been a high profile cyberattack, news coverage of most incidents is minimal, even though the threats and occurrences of such attacks are significant. The largest ransomware attack in history took place recently, affecting tens of thousands of computers in nearly 100 countries. Those affected were required to pay a specified amount of money in order to take back possession of their own information, but the damage had already been done. Once information is shared and disseminated, it can never be fully re-possessed, nor can its privacy and security be fully re-established.

It is not a coincidence that the increasing pervasiveness of cybercrime parallels the upward trajectory of technological advancements in electronic data transferability, accessibility and storage. Electronic storage of plan data has been the industry standard for quite some time, but more complex and sophisticated forms of electronic storage, including cloud storage and remote server storage, have continued to evolve at a rapid pace. Furthermore, phone applications, remote employees, third-party administrators, and IT support are data access points that increase the potential for information to be infiltrated.

Although cybercrime is listed as one of the Federal Bureau of Investigation's top priorities, cybersecurity issues, in the context of maintaining privacy and security around employee benefit plans, remain largely unaddressed. The main concerns cyberattacks raise for employee benefit plans include the unauthorized collection of personal identity and personal identifiable information ("PII"); the theft of money from bank accounts, investment funds, and retirement accounts; and the infiltration of plan administration, service provider and broker systems. In February 2015, hackers breached Anthem, Inc.'s computer system and publicly released the personal information of an estimated 80 million customers and employees. In June 2016, more than 90 deferred-compensation retirement accounts of Chicago municipal employees were breached. In July 2016, a cyberattack targeted a grocery workers union pension plan in St. Louis. These significant threats of identity theft and loss of plan assets via hacking of plan financial data emphasize the importance of reviewing, identifying and overhauling the less than rigorous cybersecurity policies and procedures most entities possessing PII have in place today. Cyberattack threats also warrant examination of the responsibilities of benefit plan fiduciaries with respect to cybersecurity.

Responsibilities of ERISA Fiduciaries

Under Section 404(a) of ERISA, a benefit plan's fiduciaries must discharge their duties to the plan solely in the interest of the participants and beneficiaries and for the exclusive purpose of providing for their benefits. These duties must be carried out with the care, skill, prudence and diligence under then-prevailing circumstances that a prudent man acting in a like capacity and familiar with such matters would use in the conduct of an enterprise of a like character and with like aims.[1] Because benefit data

includes participants' names, Social Security numbers, account information and PII, it is increasingly important for ERISA plan fiduciaries to acknowledge and act on their inherent responsibilities to secure online plan data from cyberattacks. Failure to do so would almost certainly be counter to the prudence standard by which ERISA fiduciaries are required to abide.

Pursuant to Interpretive Bulletin 96-1 (the "Bulletin"), the selection and monitoring of a benefit plan's service providers is a key fiduciary responsibility, and plan fiduciaries assume liability for the failure to act prudently in selecting service providers.[2] While the Bulletin addresses the designation of a person(s) by plan fiduciaries to provide investment educational services or investment advice to plan participants and beneficiaries, the Bulletin has been interpreted more broadly to establish the requirement of prudence in service provider selections, including prudence in the selection of a service provider that maintains electronic plan data in order to keep that plan data private and secure. Accordingly, ERISA plan fiduciaries should consider cybersecurity when selecting service providers. Unfortunately, there is no direct guidance from the Department of Labor ("DOL") on cybersecurity considerations in carrying out this important process.

Developing Best Practices In the Absence of Cybersecurity-Related ERISA Regulation

The lag to adopt cybersecurity measures by ERISA fiduciaries is likely reflective, at least in part, of the lack of on-point guidance available to plan fiduciaries on *how* to meet their obligation to keep participants' and beneficiaries' information secure.

While there is currently no comprehensive federal law governing cybersecurity, the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") establishes privacy and security measures to protect the individually identifiable health information of participants in group health plans. Although data breaches have long been a concern of health benefit plan administrators under the HIPAA, these concerns about safeguarding PII are now being shared by fiduciaries of other types of plans, including pension plans, in the wake of an unprecedented number of breaches. Arguably, it is the fiduciaries of 401(k) and other benefit plans not subject to HIPAA's privacy and security measures whose responsibilities have expanded to include the implementation and management of processes minimizing cyber risks, since health benefit plans are already required to comply with those measures. A health plan fiduciary's compliance with ERISA requires compliance with HIPAA, and therefore a HIPAA breach via disclosure of PII to unauthorized individuals could trigger a breach of ERISA's prudence standard. However, HIPAA's privacy and security requirements only require health plan sponsors to consider how potential breaches might occur and what measures should be implemented to avoid them. The mere consideration of how to protect PII is likely not enough to meet the broad fiduciary prudence standard under ERISA. As a result, data breaches and the fiduciary obligations associated with safeguarding against such breaches should be the concern of *all* plan fiduciaries equally, regardless of whether they are already subjected to HIPAA's privacy and security rules. Accordingly, it is increasingly important for any individual or entity interacting with a plan to be knowledgeable regarding the effect plan data and asset cyber breaches would have on participants and beneficiaries, as well as plan fiduciaries' duties under ERISA to implement defenses against cyber threats to PII.

The ERISA Advisory Council ("Council"), established to advise the Secretary of Labor, examined cybersecurity considerations as they relate to pension and welfare benefit plans in 2011 and revisited the issue in 2016. The 2011 Council issued a report urging the DOL to issue guidance on the obligation of plan fiduciaries to protect the PII of plan participants and beneficiaries. The 2016 Council went further, intending its report to be a reference for plan sponsors to secure benefit plan data and assets from cybersecurity risks. To date, the DOL has not taken an official position regarding the role and responsibilities of plan fiduciaries in addressing and preventing cyber risks in response to the Council reports. As a result, and due to the increasing sophistication of cyber attacks, it is not advisable for plan fiduciaries to wait for guidance from the DOL before taking all prudent actions that are necessary to safeguard benefit plan data and assets.

Best Practices

Given the broad scope of an ERISA fiduciary's obligation to act with prudence, it is in the best interest of all parties involved with ERISA plans to begin developing systems and procedures for properly handling and securing PII. The ERISA Advisory Council recommendations may represent the foundation for future regulatory or statutory efforts to address plan fiduciaries' responsibility for cybersecurity matters. As such, the Council's proposed strategies should serve as a baseline for the standard of care ERISA fiduciaries should implement when addressing such matters.

Cybersecurity issues and concerns in employee benefit administration include breaches of the information systems used in the industry, the misuse of PII and benefits that are stored in those systems, and the impact of cyber threats on plan sponsors, service providers, participants and beneficiaries.[3] Guarding against cybersecurity breaches is a complex process, and involves instituting systems that not only detect and eliminate the source of the breach, but also measure the damage done, recover any data lost, and restore the integrity of the system.

The following are some affirmative actions plan fiduciaries can take to build a framework upon which they may base a cybersecurity risk management strategy:

- Consider purchasing cyberliability insurance;
- Perform due diligence of third-party service provider systems by vetting third-party administrators' ("TPAs") cybersecurity programs and formally requesting that TPAs provide information regarding their security systems and risks;
- Review and amend agreements with service providers to ensure there are contractual provisions mandating the protection of data and allocations of liability;
- Monitor third parties and employees with access to plan data; and
- Become more informed regarding the functionality of cloud computing and remote data storage processes to better understand where PII is located in the organization's systems and how it is stored or protected.

The above action list represents just a fraction of the procedures and policies that a plan fiduciary must consider to ensure a secure data system. The consequences of a data breach are severe and will be even more so for plan fiduciaries if their failure to address cybersecurity issues is determined to be a fiduciary breach. Regardless of whether it is explicitly stated by a governing authority, plan fiduciaries are under a fiduciary obligation to secure participant data under ERISA. The best practices listed above are ways in which a fiduciary may begin to address the threat that continues to evolve in this area and determine how to fulfill their obligation.

To prudently administer their plans, plan fiduciaries should not wait for formal guidance on these issues, but rather take action as soon as reasonably possible to develop effective practices and procedures for combatting data breaches that put PII at risk.

JUNE 2017

---

1 29 U.S.C. §1104 (2011) https://www.gpo.gov/fdsys/pkg/USCODE-2011-title29/html/USCODE-2011-title29-chap18-subchapI-subtitleB-part4-sec1104.htm

2 Interpretive Bulletin 96–1; Participant Investment Education; Final Rule, Federal Register (1996), https://www.dol.gov/ebsa/regs/fedreg/final/96_14093.pdf (last visited Jun 12, 2017).

3 *Id.*

FIRM NEWS

On May 16, **Tiffany Santos** was a panelist in a webinar hosted by the American Bar Association (ABA) Joint Committee on Employee Benefits (JCEB) entitled, *Pay Me Now or Pay Me Later: How Not to Run an Employee Benefit Plan*.

On May 24, **Tiffany Santos** was a panelist in a Strafford Publications webinar entitled, *Alternative Investments in ERISA Retirement Plans: Mitigating Liability Risks for Hedge and Private Equity Funds and Pension Plan Fiduciaries*.

On May 24, **Mary Powell** and **Eric Schillinge**r were co-presenters of a webinar entitled, *ACA Repeal: Where Things Stand — And What Lies Ahead?* The AHCA, which includes eight amendments, would significantly change a number of healthcare rules that affect group health plans and their employer-sponsors.

Download the PowerPoint presentation:
http://www.truckerhuss.com/events/

On June 9, **Brad Huss** participated in a panel discussion at the PLANSPONSOR National Conference in Washington, D.C. entitled, *Learning From Litigation*. Panelists discussed steps be taken in running a compliant plan in view of recent retirement plan lawsuits and their ramifications.

On June 22, **Tiffany Santos** will moderate a panel discussion hosted by the ABA JCEB entitled, *Gearing Up in the Era of Increased HIPAA Enforcement and Cyber Security Threats.*

On July 11, **Brad Huss** will be speaking at the Western Benefits Conference in Anaheim at Workshop 27: *Wild Ride of DOL Investigations.* This session will discuss the many issues that arise during DOL investigations and how they can be resolved. If you are being investigated or are assisting your client with their investigation, this session will give you the tools to be prepared.

On July 12, **Callan Carter** will be speaking at the Western Benefits Conference in Anaheim at Workshop 40: *Fiduciary Issues with Participant Health Plan Data Privacy.* Data breaches are becoming increasingly common in the health plan world. This session will discuss the fiduciary's responsibility to prevent and respond to health plan data breaches.

The Trucker ✦ Huss *Benefits Report* is published monthly to provide our clients and friends with information on recent legal developments and other current issues in employee benefits. Back issues of *Benefits Report* are posted on the Trucker ✦ Huss web site (www.truckerhuss.com).

Editor: Shannon Oliver, soliver@truckerhuss.com