REGULATORY Update

Q3 2021

Proposed Legislation Targets Changes to Retirement Accounts

June was a busy month for lawmakers, with several pieces of new legislation introduced that are designed to enhance retirement savings opportunities for American workers. Below are the highlights of what each piece of legislation would aim to accomplish if passed.

Enhancing Emergency and Retirement Savings Act of 2021

Senators James Lankford (R-Oklahoma) and Michael Bennet (D-Colorado) introduced the Enhancing Emergency and Retirement Savings Act of 2021 on June 2. This act would provide retirement account owners some flexibility when they need to cover an emergency expense by providing a penalty-free "emergency personal expense distribution" option from employer-sponsored retirement plans and IRAs. The proposal allows for one emergency distribution per calendar year of up to $1,000 from the individual's account, with a requirement that the withdrawn funds be paid back to the plan before an additional emergency distribution from that same account is allowed. The amount can be recontributed within a three-year period to any eligible plan to which a rollover contribution can be made.

Keeping Your Retirement Act and Increasing Retirement Amount Act

Sen. John Kennedy (R-Louisiana) introduced two bills that are squarely focused on retirement savings themes. The first, the Keeping Your Retirement Act, introduced on June 7, proposes to raise the RMD age from 72 to 75 for certain retirement accounts. This, according to a press release issued by Kennedy, "would give seniors more time for their retirement savings to grow before they are required to make annual withdrawals that can deplete their savings and increase their tax liability." It is worth noting that a current bill, the Improving Access to Retirement Act (coined SECURE 2.0) was unanimously passed by the House Ways and Means Committee earlier in 2021. It is expected to be passed into law in the near future and mandates that the RMD age be raised to 75.

The second, called the Increasing Retirement Amount Act, also introduced on June 7, would allow individuals who do not have access to a workplace retirement plan to increase their IRA contributions to $12,000 per year (the current maximum IRA contribution is $6,000 per year). The legislation would allow for an additional $3,000 to be contributed per year for individuals who are at least 50 years old and who do not have a workplace retirement plan, bringing total annual IRA savings for those individuals up to $15,000.

Retirement plan sponsors and administrators should keep a watchful eye on the development of these pieces of legislation, as their passage could affect retirement plan transactions in the future.

DOL Issues Cybersecurity Best Practices for Retirement Plan Sponsors

In recent years, cybersecurity—the protection of electronic data from unauthorized and criminal use—has become a keen focus for corporations, small businesses, and individuals alike.

Recently, the [DOL weighed in] on cybersecurity for the first time by providing guidance to businesses that sponsor a workplace retirement plan. This guidance provides best practices and tips for safeguarding the sensitive personal information of employees. It aims to help protect the personal data of more than 140 million working Americans who participate in workplace defined benefit or defined contribution plans, which represents an estimated $9.3 trillion in assets.

To help retirement plan sponsors and fiduciaries organize their cybersecurity efforts, the DOL's guidance is broken into three areas of focus, which are summarized below.

Tips for Hiring Service Providers

This section of guidance offers plan sponsors and fiduciaries key tips to help them prudently select a service provider—such as a recordkeeper, third-party administrator, or custodian—with strong cybersecurity practices and monitor its activities, as required by ERISA. Some of these tips include:

- Inquiring about the service provider's information security standards, practices, and policies and how those practices are validated and maintained on an ongoing basis
- Evaluating the cybersecurity track record of service providers
- Determining whether service providers hold insurance policies that would cover losses due to cybersecurity breaches

Cybersecurity Program Best Practices

The DOL prescribes ways that plan fiduciaries and recordkeepers can manage cybersecurity risks by creating and implementing a well-documented cybersecurity program. A cybersecurity program should:

- Identify and assess internal and external cybersecurity risks that may threaten the confidentiality, integrity, or availability of stored nonpublic information
- Evaluate ongoing risk with an annual assessment
- Have a third-party audit of security controls
- Have clearly defined and assigned information security roles and responsibilities and strong access control procedures
- Conduct cybersecurity awareness training for all personnel
- Contain a plan for responding to cybersecurity incidents or breaches

Online Security Tips for Plan Participants

To provide an extra layer of defense for thwarting cyberattacks, participants and beneficiaries should be diligent and adhere to basic rules to reduce the risk of online fraud and loss. Tips to protect personal data include:

- Routinely monitoring online retirement plan accounts
- Using strong and unique passwords and multifactor authentication
- Keeping personal information updated and current
- Being wary of connecting to free Wi-Fi, which can open the door for cybercriminals to hack into personal accounts
- Knowing the signs to identifying phishing attacks (Phishing is an attempt to trick individuals into sharing passwords, account numbers, and sensitive information, usually with a suspicious message that is disguised to look like it is from a legitimate organization.)
- Using antivirus software and keeping apps current

Cybercrime is on the rise, with an estimated $4.2 billion in losses last year derived from nearly 800,000 cybercrime complaints, according to the FBI. As a good first step, business owners, retirement plan sponsors, and fiduciaries should familiarize themselves with the DOL's guidance and review it carefully with their internal information security stakeholders. Then, schedule time to speak with service providers and a retirement plan advisor to organize a plan of action to ensure that their employees' personal data and information is well-guarded.

We Can Help

We are ready to provide you with the ideas, guidance, and foresight to position your firm for success. If you would like to review how retirement plans are affected by potential legislation, the DOL's new cybersecurity guidance, or any industry happenings that may affect your firm's benefit plan offerings, we're here to assist you.

Commonwealth Financial Network® does not provide legal or tax advice. Please contact your legal or tax advisor for advice on your specific situation.

Securities and advisory services offered through Commonwealth Financial Network®, Member FINRA/SIPC, a Registered Investment Adviser.

Authored by the Retirement Consulting Services team at Commonwealth Financial Network.

© 2021 Commonwealth Financial Network®

RCS-1479-22114_07/21