CERINI & ASSOCIATES, LLP | CERTIFIED PUBLIC ACCOUNTANTS
*PRESENTS*

# PENSION PLANNER

VOL. 4
SUMMER 2021

## SECURE ACT 2.0

## IS IT TOO SOON FOR CRYPTO TO COME TO THE 401(K)?

## THERE'S NO TIME TO WAIT: PLAN SPONSORS MUST UPDATE CYBERSECURITY PRACTICES NOW

BRINGING A UNIQUE UNDERSTANDING OF KEY ISSUES FACING BENEFIT PLANS

## FROM THE EDITOR - TANIA QUIGLEY, CPA

We normally issue our pension planner newsletter annually, but we felt the importance of bringing the information in these articles to your attention sooner than waiting months to include in the next volume.

Cybersecurity is a hot topic in all industries and is now a focus of the Department of Labor. Cybersecurity is a risk that all plan sponsors must consider if they haven't already. It's become so important to have a cybersecurity plan in place and to educate and train your employees of the risks of security breaches and make sure they are aware of your cybersecurity policy. Plan sponsors also have the responsibility to ensure service providers (*TPA's and Plan Custodians*) also have sufficient cybersecurity policies in place. The article provides some helpful information for questions to ask service providers and things you need to do to help protect your Plan's assets.

*Who knew cryptocurrency and retirement plan investments would be in the same sentence?* As cryptocurrency becomes an increasingly popular investment, it's an investment option that some plans may decide to consider. As expected, there are risks that come with such a highly volatile investment.

Finally, retirement plans have been spotlighted by regulation changes to improve accessibility and retirement benefits for participants. Just when you have familiarized yourself and implemented the SECURE Act into your pension plan, there is another round of regulation changes in the works, referred to as SECURE Act 2.0. This second round of the SECURE Act will benefit employees that may not be able to contribute, will make pension plans more accessible to employees through mandatory auto-enrollment, provide some businesses with tax benefits to start up a plan for its employees, increase contributions for employees nearing retirement age, and makes changes to annuity and required minimum distribution regulations. Savings for the future through means of a retirement plan has always been encouraged but it's become more evident through these proposed regulation changes that bring the importance of retirement savings to light.

Plan sponsors have a fiduciary responsibility to their employees to properly safeguard and administer plans. With all of the other responsibilities that you have, we realize you don't always have the time to stay up on regulatory changes and shifting risks. Don't worry, we got your back. Please reach out to us if you have any questions or if we can be of any help.


### CONTRIBUTORS

**EDITOR**
TANIA QUIGLEY, CPA
CERINI & ASSOCIATES, LLP
PARTNER, AUDIT

**WRITERS**
ERIN GRUPPE
CERINI & ASSOCIATES, LLP
STAFF ACCOUNTANT

THOMAS ALLEN
CERINI & ASSOCIATES, LLP
STAFF ACCOUNTANT

JENNY L. HOLMES
NIXON PEABODY
ASSOCIATE | DEPUTY LEADER, CYBERSECURITY & PRIVACY

**ASSOCIATE EDITOR**
KEN CERINI, CPA, CFP, FABFA
CERINI & ASSOCIATES, LLP
MANAGING PARTNER

**PAGE LAYOUT & DESIGN**
KRISTINA (LAINO) TORTORICE
CERINI & ASSOCIATES, LLP
GRAPHIC DESIGNER



3340 VETERANS MEMORIAL HWY., BOHEMIA, NY 11716 | (631) 582-1600 | WWW.CERINICPA.COM


# SECURE ACT 2.0

Retirement plans have experienced some regulation changes over the past year thanks to the SECURE Act. The SECURE Act was put into place to make retirement plans more accessible and beneficial to participants and employers. There is a new bill going through Congress that will add more changes to retirement plan regulations, called Securing a Strong Retirement Act or SECURE Act 2.0. Here are highlights in the bill:

### STUDENT LOANS AND RETIREMENT SAVINGS:

Employees paying down student loan debt may not have the financial ability to contribute into a retirement plan. The bill will allow employers to contribute to its employees' retirement account who are not contributing and paying student loan debt. This arrangement applies to employers that make a match contribution on behalf of their employees. The match would be equal to the amount of the student loan payment, up to a certain percentage of the employee's compensation.

### INCREASE CATCH-UP CONTRIBUTIONS:

The current rules allow for individuals over age 50 to have the ability to contribute an additional $6,500 into their retirement account, called a catch-up contribution. This bill will allow for an additional catch-up contribution of $10,000 into a 401(k) or 403(b) plan or $5,000 into a SIMPLE IRA for individuals over the age of 60. The bill also allows for annual adjustments for inflation for catch-up contributions to an IRA plan.

### REQUIRED MINIMUM DISTRIBUTIONS:

As people are living and working longer, the SECURE Act recognized the need to increase the required minimum distribution age from 70½ to 72. The bill will increase the age limit to 75. In addition, retirees with less than $100,000 in retirement savings could be excluded from taking these required minimum distributions.

### ANNUITY INVESTMENTS:

Individuals that select an annuity arrangement are set up to receive guaranteed payments over a specific period of time. These annuity arrangements are currently subject to limitations. Such limitations are eased in the bill and will make it easier for plans to offer annuities and allow for Qualified Longevity Annuity Contracts which can increase the amount of retirement savings allowed to be used.

### AUTO-ENROLLMENT:

Auto-enrollment is an option for employers to adopt in its 401(k), 403(b) or SIMPLE IRA plans. This bill will require the auto-enrollment feature to be mandatory for all newly eligible employees. The withholding rate will be 3% from the employee's pay, increasing each year by 1% until employee reaches 10% withholding rate.

### SAVER'S CREDIT:

The saver's credit, which allows for a tax credit to lower-income individuals that save for retirement. The bill would increase the credit to 50% of the amount contributed, which increases the value of the credit from $1,000 to $1,500.

### EMPLOYER SAVINGS:

Setting up a retirement plan can be costly to small businesses. Currently, there is a three-year 50% tax credit businesses can take for the administrative costs of setting up a retirement plan. Businesses that qualify will have up to 50 employees. The bill will increase the tax credit to 100% and may allow defined contribution plans (*i.e. 401(k) plans*) to receive higher credits. Plan paperwork is another administrative responsibility of the employer. Currently, participants are required to receive several documents and disclosures regarding the retirement plan with their employer. The bill would no longer require the sending of these disclosures, other than the employer notifying the employee that they can enroll in the retirement plan. The bill would place the responsibility of simplifying these reports and disclosure requirements in the hands of the US Treasury, Department of Labor, and the Pension Benefit Guaranty Corporation. Lastly, penalties will be lessened for some reporting mistakes made by the employer.


**ERIN GRUPPE**
*STAFF ACCOUNTANT*


# IS IT TOO SOON FOR *CRYPTO TO COME TO THE 401(K)?*

Cryptocurrencies have increasingly gained traction throughout the last decade. As technology progressed, cryptocurrency, or crypto for short, has gained momentum as not only a medium for exchange, but also as an investment opportunity. There are thousands of different types of cryptocurrencies, however, you most likely heard of at least one of these three types of crypto tokens: Bitcoin, Ethereum, and XRP.

The relatively rapid price appreciation of such digital currencies has turned heads. Think about this, Bitcoin was worth less than a penny back in 2009. Throughout May to June of the 2021 market period, Bitcoin has surpassed $30,000 for one token. Market demand has driven the price sky-high, as both individual investors and firms have flocked to the cryptocurrency market.

Buyers have been able to enter the market through applications that contain a *"digital wallet."* Think of these apps where the buyer transfers real money to buy cryptocurrencies. Beyond this method of investing, consumers have been limited. As more interest has formed regarding crypto, an increasing number of investment firms aim to get a piece of the pie. However, one in particular has proposed merging both the crypto and retirement markets.

ForUsAll, a small 401(k) provider, will soon be allowing investors to allocate up to 5% of their investable assets into crypto. Using Coinbase, a cryptocurrency exchange app, as their partner, the investment firm aspires to give everyday investors the ability to make crypto a part of their investment portfolio. As of now, the company is offering both a traditional and Roth 401(k) to allow individual taxpayers to save for retirement while investing in cryptocurrency.

Regardless of the type of retirement account these prospective consumers choose, the question really is, *do cryptocurrencies belong in retirement accounts?* The short answer is that it depends. Each investor is unique and needs to evaluate the information available to properly weigh risks. Here are just a few things to consider:

### 1. *Cryptocurrency is largely unregulated.*

Many cryptocurrencies such as Bitcoin or Ethereum, remain unregulated by the Securities and Exchange Commission, or the SEC for short. Conversely, ETFs and mutual funds, commonly found in 401(k) products, are subject to such regulations.

### 2. *The Cryptocurrency market is highly volatile.*

The reason why the pricing of most cryptocurrencies are extremely volatile is that many tokens, including Bitcoin, are scarce in quantity and these coins are not managed by a central bank. Like any currency, for an individual to turn a profit, someone else subsequently has to pay more for the currency than the person before them. Think of the *"Greater Fool Theory,"* which argues that price appreciation happens through selling an overpriced asset to the next person. This cycle perpetuates until there are no buyers left in the market. This will subsequently cause a major sell-off, in other words, a significant price decrease.

### 3. *Remember in 2008, when people were issued debit cards for their 401(k)'s? Is this yet another example of overcomplicating 401(k)'s?*

Back in 2008, when employees invested in a 401(k), some companies began to issue these so-called *"debit cards."* In reality, these *"debit cards"* worked more like credit cards. The money that was charged against a 401(k) was treated as a loan against the account, which was subject to early withdrawal fees, interest, and penalties. *Will crypto follow suit in overcomplicating the 401(k) by adding yet another asset class?* The answer is too early to tell. When examining crypto, there is not enough market history to predict if this is will be a profitable investment for the long term.

### 4. *The issue of liquidity with a 401(k).*

Due to the volatile nature of cryptocurrencies, the price fluctuations are massive. If an employee wanted to sell their coins in their retirement account before they meet the minimum age to withdraw penalty-free, they are likely to pay more in taxes and fees than investing in crypto using conventional methods, such as using an application like Coinbase.

Right now, the use of crypto in the IRA market remains highly exclusive, as large retirement investment firms still refrain from using it as an asset class in their employee retirement portfolios. Due to its volatility and lack of regulations, it is unclear if Bitcoin, or any other token, will become a viable investment choice for your retirement plan. Remember, as an employer, you have a fiduciary responsibility to your employees … so consider carefully should your pension company allow crypto options within your plan.

**THOMAS ALLEN**
*STAFF ACCOUNTANT*

# THERE'S NO TIME TO WAIT: PLAN SPONSORS MUST UPDATE CYBERSECURITY PRACTICES NOW

In April, the **Department of Labor (DOL)** issued its first guidance on cybersecurity practices for ERISA retirement plans. The guidance, which was largely in response to a US Government Accountability Office report urging the DOL to issue cybersecurity recommendations, establishes the DOL's minimum expectations for addressing cybersecurity risks.

The guidance was issued in three parts: **(i)** *Cybersecurity Program Best Practices;* **(ii)** *Tips for Hiring a Service Provider with Strong Cybersecurity Practices;* and **(iii)** *Online Security Tips*. While all three parts of the guidance include tips and best practices, plans must make sure their practices and procedures are memorialized.

The first two parts of the guidance intend to help plan sponsors manage cybersecurity risks, including how to prudently select service providers. The Cybersecurity Program Best Practices offers twelve action items that plan sponsors and plan service providers should do. This includes having a formal, well-documented cybersecurity program, conducting an annual risk assessment, and implementing strong controls to protect the data. The third piece provides tips for plan participants and beneficiaries to reduce the risk of loss, such as using unique passwords and multi-factor authentication.

Generally, when the DOL or other regulators issue guidance like this, we would not expect to see audit activity for at least a year or two. However, we are already aware of several investigations that the DOL has commenced regarding cybersecurity practices. We are reproducing requested documentation in one such investigation.

*So what should plan sponsors do in response to these guidelines?*

## CREATE OR REVIEW A WRITTEN CYBERSECURITY PROGRAM

As an initial matter, plan sponsors should take a step back and analyze their cybersecurity program as a whole, reviewing any policies that are in place and identifying any gaps. Once gaps or weak areas are known, plan sponsors can begin the process of creating or updating a written cybersecurity program.

The DOL lists eighteen areas that a comprehensive program should govern, including: **(i)** *data governance and classification,* **(ii)** *access controls and identity management,* **(iii)** *data disposal,* **(iv)** *incident response,* **(v)** *encryption,* and **(vi)** *cybersecurity awareness training.* Additionally, the DOL recommends conducting annual risk assessments and third-party audits to test the effectiveness of the written program. The DOL makes clear that as part of an audit, it would expect to see audit reports, penetration test reports, and other analyses of the party's cybersecurity practices.

The DOL also emphasizes the importance of having clearly defined roles and responsibilities. In other words, plan sponsors need to designate an individual or team to maintain the cybersecurity program. This may include creating a cross-functional team that can make and implement decisions relating to cybersecurity.

## MAKE A PLAN FOR VENDOR DILIGENCE AND MANAGEMENT

As part of the formal cybersecurity program, plan sponsors should establish a plan for selecting and managing service providers. The DOL provides tips for hiring a service provider with strong cybersecurity practices. These tips aim to help plan sponsors and fiduciaries to prudently select service providers and to monitor their activities. This guidance offers six tips for plan sponsors looking at engaging with a service provider to ensure that the service provider has thorough cybersecurity practices:

1. Ask about the service provider's information security standards, practices, and policies, and audit results, and compare them to the industry standards adopted by other like institutions. Plan sponsors should look for service providers that follow a recognized standard for information security.
2. Ask the service provider how it validates its practices and what levels of security standards it has met and implemented.
3. Evaluate the service provider's track record in the industry, including public information regarding information security incidents, litigation, or other legal proceedings related to the offered services.
4. Ask whether the service provider has experienced any past security breaches. If it has, ask for details, including what the service provider did in response.
5. Determine if the service provider has any insurance policies that would cover losses caused by cybersecurity incidents, including identity theft breaches.
6. Require contracts with a service provider to include ongoing compliance with cybersecurity and information security standards.

Additionally, plan sponsors should consider developing contractual provisions obligating the service providers to maintain strong cybersecurity practices. For example, plan sponsors should require service providers to regularly conduct third-party audits to determine compliance with information security policies and to meet all applicable cybersecurity and privacy laws. Service providers should be contractually prohibited from using or sharing the information for any other reason or without the plan sponsor's consent. Plan sponsors should also require quick notice of cyber incidents affecting plan data and the contract should clearly designate responsibilities for notification and associated costs and should require insurance coverage with limits high enough to reimburse for a security breach.

## PREPARE PLAN PARTICIPANTS

The DOL also contemplates ways to help plan participants who check their retirement plan accounts online to protect themselves against the risk of fraud and loss. For example, the DOL recommends plan participants use strong and unique passwords as well as take advantage of multi-factor authentication, where applicable. Plan participants should keep personal contact information current and take the time to close or delete unused accounts.

The responsibility is not specifically placed on plan sponsors to educate plan participants on cybersecurity best practices, but it is certainly in plan sponsors' best interests to provide trainings and resources to plan participants. While plan participants can be a point of access for hackers to gain entry to plan information, they can also act as a strong line of defense. Having cybersecurity-savvy participants can be just as beneficial as a strong written cybersecurity program. Cybersecurity is not infallible. Incidents will happen. What's important—and what we believe the DOL will want to see—is the effort to prioritize cybersecurity. And given the recent audit activity, creating (*or reviewing*) your comprehensive cybersecurity program should be done sooner rather than later.

## EXAMPLE DOL AUDIT QUESTIONS:

1. All policies, procedures, or guidelines relating to:
   a. *Data governance, classification, and disposal*
   b. *The implementation of access controls and identity management, including any use of multi-factor authentication*
   c. *The processes for business continuity, disaster recovery, and incident response*
   d. *The assessment of security risks*
   e. *Data privacy*
   f. *Management of vendors and third-party service providers, including notification protocols for cybersecurity events and the use of data for any purpose other than the direct performance of their duties*
   g. *Cybersecurity awareness training*
   h. *Encryption to protect all sensitive information transmitted, stored, or in transit*
2. All documents and communications relating to any past cybersecurity incidents
3. All security risk assessment reports
4. All security control audit reports, audit files, penetration test reports and supporting documents, and any other third-party cybersecurity analyses
5. All documents and communications describing security reviews and independent security assessments of the assets or data of the Plan stored in a cloud or managed by service providers
6. All documents describing any secure **system development life cycle (SDLC)** program, including penetration testing, code review, and architecture analysis
7. All documents describing security technical controls, including firewalls, antivirus software, and data backup
8. All documents and communications from service providers relating to their cybersecurity capabilities and procedures
9. All documents and communications from service providers regarding policies and procedures for collecting, storing, archiving, deleting, anonymizing, warehousing, and sharing data
10. All documents and communications describing the permitted uses of data by the sponsor of the Plan or by any service providers of the Plan, including, but not limited to, all uses of data for the direct or indirect purpose of cross-selling or marketing products and services

Please note that you may need to consult not only with the sponsor of the Plan, but with the service providers of the Plan to obtain all documents responsive to these requests. If you are unable to produce documents responsive to any of the forgoing, please specify the requests and the reasons for the non-production.

**JENNY L. HOLMES**
*ASSOCIATE*
*DEPUTY LEADER, CYBERSECURITY & PRIVACY*
NIXON PEABODY

# CERINI & ASSOCIATES LLP

## CERTIFIED PUBLIC ACCOUNTANTS



**Industries Served**

*Construction • Real Estate • Healthcare*
*Manufacturing • Technology*
*Professional Services • Consumer Services*
*Inbound Internal Businesses • Emerging Startups*

**Cerini & Associates, LLP**
P: (631) 582-1600 | F: (631) 582-1714 | W: www.cerinicpa.com | 3340 Veterans Memorial Hwy., Bohemia, NY 11716