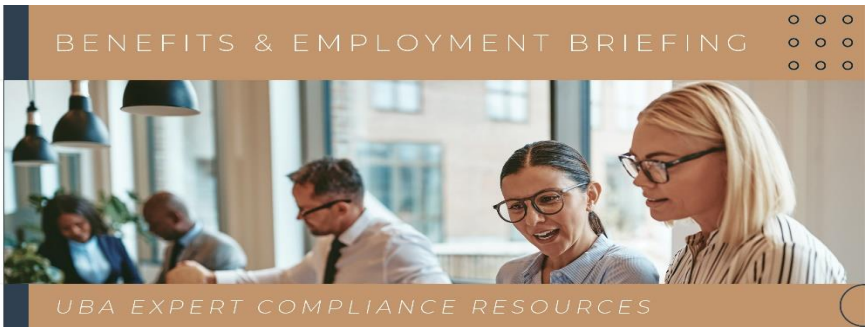
COMMONWEALTH BENEFITS GROUP

UBA PARTNER FIRM | Shared Wisdom. Powerful Results.®



Stay compliant with Benefits & Employment Briefing

Welcome to the UBA Partner Firm exclusive quarterly newsletter delivering insights about employee benefits and labor law compliance.

Benefits & Employment Briefing | Spring 2022

EBSA to Monitor 401(k) Cryptocurrency Investments

Employees and retirees have begun to press their employers to include cryptocurrency among available 401(k) investment options. The Employee Benefits Security Administration (EBSA) recently warned it will scrutinize such investments to make sure plans maintain proper oversight. EBSA further cautioned plan sponsors to be extremely careful when deciding whether and how to incorporate cryptocurrency as an investment option.

EBSA's informal guidance does not bar 401(k) plans from including crypto, but it does mean plan fiduciaries will need to conduct a thorough evaluation before offering it. Further, plan sponsors should anticipate EBSA investigating if a plan includes such an option. What do employers need to know about the recent guidance, and what should they do if weighing cryptocurrency-based 401(k) investments?

Background

President Biden recently issued an Executive Order outlining a national digital asset policy that calls on federal regulators to emphasize consumer and investor protection in the cryptocurrency space. Almost immediately, EBSA issued Compliance Assistance Release No. 2022-01 (Release) in which it reminded plan fiduciaries of

their duty to act solely in the financial interests of plan participants. The guidance included a candid warning that the EBSA expects to launch a program targeting plans that offer participant investments in cryptocurrencies and crypto-related products, and to take "appropriate action" to protect plan participants and beneficiaries. We cannot speculate as to the scope of the program or the severity of related penalties, but plan sponsors undoubtedly should act cautiously in this space.

EBSA's Authority

Pursuant to the Employee Retirement Income Security Act of 1974 (ERISA), EBSA can investigate employee benefit plans to protect the interests of plan participants and beneficiaries. EBSA has the power to subpoena documents and to compel the attendance and testimony of witnesses. Further, if EBSA believes that plan fiduciaries have violated their fiduciary duties or engaged in prohibited transactions, it can refer the matter to the Department of Labor's Solicitor's Office to file a federal civil suit for monetary and injunctive relief. EBSA also conducts investigations of potential criminal violations of ERISA, which the Department of Justice can prosecute.

Retirement plan fiduciaries owe the duties of skill, prudence, and diligence to plan participants and beneficiaries and, for example, must diversify a menu of investment options offered in a 401(k) plan. In addition, the Supreme Court in *Hughes v. Northwestern University* recently reminded plan fiduciaries of their continuing duty to monitor 401(k) plan investments and to remove any imprudent investment options. An investment can be imprudent for several reasons, including undue risk and excessive fees and costs.

EBSA highlighted several focal points including the volatility, valuation complexities, and unique custody and recordkeeping aspects of digital assets compared to more traditional investments. It also expressed concern that plan participants may not be equipped to make informed investment decisions regarding digital assets such as cryptocurrencies. Given these statements, EBSA's investigations will likely evaluate the prudence of digital assets, including cryptocurrencies, as possible 401(k) plan options.

Plan sponsors should keep in mind that EBSA can initiate an investigation based on complaints from participants or service providers, media reports, and data collected from annual plan filings. EBSA will also conduct investigations pursuant to specific enforcement initiatives that focus on a particular area of concern – like cryptocurrency. Moreover, EBSA can expand its investigation beyond a single benefits plan, and can include service providers in its review. If, upon investigation, EBSA believes that a particular digital asset investment option in a 401(k) plan is imprudent, the Solicitor's Office may file a lawsuit against the fiduciaries of the plan in federal court. EBSA also issues civil monetary penalties equal to 20% of any money recovered. In addition, fiduciaries who breach their duties of professional care can be held personally liable for any losses to the plan resulting from the breach.

What to do now

Employers or financial institutions that offer cryptocurrencies under 401(k) plans should thoroughly weigh the risks and benefits of doing so. As with all investment options, employers and other fiduciaries should continue to monitor and evaluate the prudence of each cryptocurrency included as investment options. Lastly, whether you are an employer, fiduciary, or a service provider to a 401(k) plan, you should immediately seek the assistance of legal counsel if you receive a letter or subpoena from EBSA.

Transparency Rules Require Plan Sponsors to Act Now Before July 1 Deadline

The Departments of Health and Human Services, Labor, and Treasury (the Departments) released Transparency in Coverage (TiC) rules in late 2020 that will require fully insured and self-funded plan sponsors of non-grandfathered group health plans to make important disclosures about in-network and out-of-network rates beginning July 1, 2022. To be ready to meet that deadline, plan sponsors should be coordinating efforts with carriers and third-party administrators (TPAs), as the case may be, to ensure they have the necessary information in the proper format to comply with the new TiC requirements.

Devil in the Details

The TiC rules originally required certain employers to provide "machine readable" files that disclose in-network rates, out-of-network charges and information relating to prescription drug coverage and costs by January 1, 2022. Last year the Departments delayed enforcement of the prescription drug coverage rules indefinitely until they issue additional guidance. However, plan sponsors should be taking steps now to ensure they can publish the required in-network negotiated rates and out-of-network allowed amounts as laid out in the TiC rules by the new July 1 deadline.

The first required file (In-Network Rate File) must show a plan's negotiated rates for all covered items and services between the plan or carrier and all in-network providers. The second file (Allowed Amount File) will show both the historical payments to, and billed charges from, out-of-network providers. Plan sponsors must be sure this file includes at least 20 historical entries to safeguard individual privacy. The departments have indicated they will provide more specific guidance as to format and content, but so far have not released more details than what we know from the final rules.

Machine-Readable Files

The machine-readable files must include:

- For each option a group medical plan or carrier offers, the identifier for each such option. The identifier is either the insurer Health Insurance Oversight (HIOS) identifier, or if the plan or insurer does not have a HIOS number, the employer identification number (EIN).
- A billing code, which can include a Current Procedural Terminology (CPT) code, Healthcare Common Procedure Coding System (HCPCS) code, Diagnosis-related Group (DRG) code, or a National Drug Code (NDC) or any other common payer identifier. This content element also requires a plain language description for each billing code of each covered item or service.

In-Network Rate File

The In-Network Rate File must show:

- In-network rates for each item or service provided by in-network providers, including any negotiated rates, fee schedule rates used to determine cost-sharing, or derived amounts, whichever rate is applicable to the plan.

- If a rate is percentage-based, include the calculated dollar amount, or the calculated dollar amount for each National Provider Identifier (NPI) identified provider, if rates differ by providers or tiers. Bundled items and services must be identified by relevant code.

Allowed Amount File

The Allowed Amount File must show:

- Unique out-of-network allowed amounts and billed charges with respect to covered items or services, furnished by out-of-network providers during the 90-day period that begins 180 days prior to the publication date of the file.
- The plan or insurer must omit data for a particular item or service and provider when the plan or insurer would be reporting on payment of out-of-network allowed amounts for fewer than 20 different claims for payment under a single plan or coverage. These amounts must also be expressed as dollar amounts and associated with the NPI, Taxpayer Identification Number, and Place of Service Code for each network provider

What Should You Do?

Plan sponsors will need to update the information in the required files no less frequently than monthly. This will likely require strong coordination with the carrier in an insured plan and with the TPA in a self-funded plan.

The Departments will require the files to be posted to a public website that consumers can use without providing individually identifiable information. The website should be open access and not require passwords, account setup, login credentials or any other barriers to accessing the required information.

The TiC rules recognize that a plan sponsor might not have its own public website on which it will be able to house the required files. But the rules permit plan sponsors to contract with a carrier, TPA or other third party to produce and house the information on a plan's behalf. However, plans should be aware that they might ultimately remain responsible for any failures.

A carrier will be responsible for any failure if a plan has required it in writing to ensure a plan's compliance. Self-funded plans can contract to have another entity provide and update required files, too, but the TiC rules do not provide the same level of protection for any failures by a third party in the self-funded context, so plans should be sure to review relevant indemnification provisions in any third-party vendor service agreement.

Many carriers and TPAs have begun reaching out to employer plan sponsors offering to assist in in providing, preparing, updating, and hosting the required files. Employers should be carefully reviewing their service agreements and related contracts to make certain they include specific provisions dealing with all aspects of the required transparency disclosures.

Conclusion

We will continue to monitor the guidance we expect to be coming soon as to certain administrative requirements regarding formatting and hosting of the required forms and provide updates as needed.

Employers Providing Group Health Coverage to Illinois Employees Face Added Disclosure

A relatively new state law imposes a new disclosure requirement on employers that offer group health insurance to their Illinois employees – and the breadth of this requirement might catch you by surprise. The Illinois Consumer Coverage Disclosure Act (ICCDA) requires employers to provide any Illinois employees with a new notice that compares the benefits offered under the employer's group coverage with so-called essential health benefits (EHBs) required through the state's *Get Covered Illinois* marketplace. At first blush, one might think employers located outside of Illinois need not worry about the ICCDA. However, the law applies to employers of any size regardless of where they are located, so long as they have employees in Illinois who have group health coverage through a plan – fully insured or self-funded – offered by the employer.

What is Required?

Covered employers must provide a list of plan benefits and exclusions under their group health insurance plans. This must be provided in a user-friendly format that will allow individuals to easily compare plan benefits to the EHBs that must be included in qualified individual health insurance coverage available on the state's Marketplace.

The notice must address:

- Emergency services
- Hospital care
- Ambulatory patient services
- Pregnancy, maternity, and newborn care
- Prescription drugs
- Laboratory services
- Mental health and substance use disorder services, including behavioral health treatment
- Pediatric services, including dental and vision care
- Preventive and wellness services
- Chronic disease management

The Illinois Department of Labor recently published a table that highlights the elements employers must disclose to satisfy the ICCDA.

Details

The ICCDA requires affected employers to provide a notice to any plan-eligible Illinois employee hired after August 27, 2021. Employers also must provide notices annually starting in 2022, as well as provide a notice upon an individual's request. Employers can provide notices via email or by posting to an internal web portal or other electronic site that employees can access.

The IDOL has discretion to review the facts and circumstances of each case to decide the appropriate penalty amount, but it has set base penalties for employers with fewer than four Illinois employees at $500 for a first offense, $1,000 for a second offense and $3,000 for each offense thereafter. Higher amounts ($1,000, $3,000 and $5,000, respectively) apply to employers with at least four employees.

What Should You Do?

Employers who provide insured group health coverage to Illinois employees should confirm with their carriers whether they will help employers comply or will be providing notices on an employer's behalf. Employers with self-funded plans may be able to coordinate with their third-party administrators, or they can access the model information provided at the IDOL website. Employers should confirm that any carrier or TPA that agrees to provide notices does so because the penalties will fall on the employer if the carrier or TPA does not comply.

HHS Hikes the Price for HIPAA and Medicare Secondary Payer Violations

The U.S. Department of Health and Human Services (HHS) recently published its annual inflation-adjusted civil monetary penalty amounts. The higher amounts will apply to penalties assessed after March 17, 2022, for any violations occurring on or after November 2, 2015.

Health Insurance Portability and Accountability (HIPAA). HIPAA contains provisions that ensure portability of health coverage as well as protect the privacy and security of certain individually identifiable protected health information (PHI). Additionally, HIPAA requires employers to report data breaches of unsecured PHI. HHS has adopted a tiered penalty system based on the degree and nature of HIPAA a violation as follows:

Tier 1 – Lack of Knowledge

Minimum penalty is now $127 per violation, with a maximum penalty of $63,973 per violation. HHS has set the new annual penalty cap for Tier 1 violations at $1,919,173.

Tier 2 – Reasonable Cause and Not Willful Neglect

Minimum penalty is now $1,280 per violation, with a maximum penalty of $63,973 per violation. HHS has set the new annual penalty cap for Tier 2 violations at $1,919,173.

Tier 3 – Willful Neglect, Corrected within 30 Days

Minimum penalty is now $12,794 per violation, with a maximum penalty of $63,973 per violation. HHS has set the new annual penalty cap for Tier 3 violations at $1,919,173.

Tier 4 – Willful Neglect, Not Corrected within 30 Days

Minimum penalty is now $63,973 per violation, with a maximum penalty of $1,919,173 per violation. HHS has set the new annual penalty cap for Tier 4 violations at $1,919,173.

Keep in mind that HHS did announce in 2019 that it would exercise its enforcement discretion to apply lower annual caps for violations in Tiers 1 to 3. The lower caps, which are adjusted annually for inflation, were set at $25,000, $100,000, and $250,000, respectively.

Medicare Secondary Payer (MSP) Rules

The MSP rules establish an ordering system under which Medicare will pay only after (or secondary to) group health coverage sponsored by an employer with 20 or more employees. Thus, the MSP rules contain penalties to

discourage employers from forcing individuals off otherwise primary health coverage. The rules forbid employers from taking into account a current employee's (or current employee's immediate family member's) Medicare eligibility for purposes of health plan coverage. In particular, the MSP rules prohibit an employer from offering any incentive for an individual to opt out of employer-provided group health coverage in favor of Medicare. The new penalty amount for improperly incentivizing a Medicare-eligible person not to enroll in a group health plan that would otherwise be the primary medical expense payer is $10,360 per violation. These amounts add up quickly, especially as HHS views each impermissible offer of an incentive to be a separate violation.