SEI Trust Company

Quarterly Update
March 31, 2022

REGULATORY/LEGAL UPDATE

In an effort to keep you updated on changing regulations, requirements and litigation that may affect our industry, we are providing you with a summary of recent legislation, legal decisions and/or regulatory guidance that may impact collective investment trusts ("CITs") and their service providers, such as banks and investment managers.

Regulatory Update

- **The DOL Takes a Strong Stance in the Cryptocurrency Debate.**

  On March 9, 2022, President Biden issued an Executive Order on *Ensuring Responsible Development of Digital Assets* ("Executive Order"), which was the Biden Administration's announcement of an intent to develop an aligned US approach across the various impacted agencies. Although the Executive Order did not explicitly reference benefit plans, it contemplates a role for the Secretary of Labor in the regulation of digital assets.

  The following day, the Department of Labor's Employee Benefits Security Administration ("DOL") issued Compliance Assistance Release No. 2022-01, entitled *401(k) Plan Investments in Cryptocurrencies* (the "Release"),[1] which "cautions plan fiduciaries to exercise **extreme** care before they consider adding a cryptocurrency option to a 401(k) plan's investment menu for plan participants" (emphasis added).

  Most importantly in the Release, the DOL threatens to investigate fiduciaries that make cryptocurrencies and related products available to their 401(k) plans. Specifically, the Release states:

  "[The DOL] expects to conduct an investigative program aimed at plans that offer participant investments in cryptocurrencies and related products, and to take appropriate action to protect the interests of plan participants and beneficiaries with respect to these investments. The plan fiduciaries responsible for overseeing such investment options or allowing such investments through brokerage windows should expect to be questioned about how they can square their actions with their duties of prudence and loyalty in light of the risks described above."

  This is a highly unusual step as the DOL does not generally make such strong admonitions around specific investment strategies or asset classes for ERISA governed retirement plans. And although not said explicitly, the DOL appears to have a presumption of imprudence for a plan fiduciary that invests plan assets into such asset classes or allows participants to direct their balances into these asset classes. Specifically, the DOL stated the following concerns about crypto-assets:

  (1) Crypto-assets are highly speculative and volatile;
  (2) There is not enough information to permit regular plan participants to make an informed decision;
  (3) There are custodial and recordkeeping concerns that have not been adequately addressed yet;
  (4) There are valuation concerns that have not been fully addressed yet.
  (5) Finally, the regulatory environment is still in flux and it is difficult to assess what happens when other regulatory agencies get involved.

  It is important to know that the Release is not law, but it does state a specific material risk for plan fiduciaries who select such assets for their ERISA governed plans, as DOL exams can typically last years and will

[1] 401(k) Plan Investments in Cryptocurrencies. https://info.groom.com/25/1004/uploads/compliance-assistance-release-no.-2022-01.pdf

consume valuable corporate resources to defend.

- **The SEC proposes 4-day reporting window for cyberattack**

  On March 9, 2022, the SEC proposed amendments to "enhance and standardize disclosures regarding cybersecurity risk management strategy, governance and incident reporting by public companies."[2]

  First, the amendments would require public companies to include disclosures on the Form 10-K about a company's cybersecurity risk management systems, including its policies and procedures for identifying, assessing, and managing the risks. Those disclosures would require, if applicable, whether the company engages third parties to assess its cybersecurity risk program and disclosures on the company's policies and procedures to oversee and identify the cybersecurity risks associated with its use of any third-party service provider, among other disclosures.

  Next, if adopted as proposed, the amendments would require public companies to report, via Form 8-K, material cybersecurity incidents within four business days after a determination that an incident has occurred. The disclosure timeframe starts when a determination of materially is made, and not when the incident is initially discovered, so there is some level of time built into the proposal to permit the company to investigate the incident, to some degree. The proposed rule also contains a non-exhaustive list of what might trigger a reporting requirement, which includes the following:

  1. an unauthorized incident that compromises the confidentiality, integrity, or availability of data, a system, or a network, or violates the company's security policies or procedures;
  2. an unauthorized incident that causes degradation, interruption, loss of control, damage to, or loss of operational technology systems;
  3. an incident in which an unauthorized party accesses (or a party exceeds authorized access) and alters, or has stolen, sensitive business information, personally identifiable information, intellectual property, or information that has resulted, or may result, in a loss or liability for the company;
  4. an incident in which a malicious actor offers to sell or threatens to publicly disclose sensitive company data; or
  5. an incident in which a malicious actor demands payment to restore company data that was stolen or altered.

  Further, the proposed rule also includes requirements for the company to provide periodic update reporting, which could be included in the company's Form 10-Q or 10-K. Again, a non-exhaustive list of potential scenarios that would require updated reporting are: incidents that have a material impact or potential material impact of the incident on the company's operations or financial condition, whether the company has remediated the incident, and any changes in the company's policies and procedures resulting from the cybersecurity incident and how the incident may have informed such changes.

  The proposed rules have entered a public comment phase that will end on May 8, 2022 at the earliest.

About SEI's Investment Manager Services Division

SEI's Investment Manager Services Division supplies investment organizations of all types with the advanced operating infrastructure they must have to evolve and compete in a landscape of escalating business challenges. SEI's award-winning global operating platform provides investment managers and asset owners with customized and integrated capabilities across a wide range of investment vehicles, strategies and jurisdictions. Our services enable users to gain scale and efficiency, keep pace with marketplace demands, and run their businesses more strategically. SEI partners with more than 550 traditional and alternative asset managers, as well as sovereign wealth funds and family offices, representing nearly $30 trillion in assets, including 49 of the top 100 asset managers

[2] SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies at https://www.sec.gov/news/press-release/2022-39

worldwide*. For more information, visit seic.com/ims.

*Based on Pensions & Investments' "Largest Money Managers" 2019 ranking.

About SEI Trust Company

SEI Trust Company (STC) is a non-depository trust company chartered under the laws of the Commonwealth of Pennsylvania that provides trust and administrative services for various collective investment trusts. SEI Trust Company is a wholly-owned subsidiary of SEI Investments Company (SEI). For more information, visit www.seic.com/stc.

About SEI

SEI (NASDAQ:SEIC) delivers technology and investment solutions that connect the financial services industry. With capabilities across investment processing, operations, and asset management, SEI works with corporations, financial institutions and professionals, and ultra-high-net-worth families to solve problems, manage change and help protect assets—for growth today and in the future. As of March 31, 2022, SEI manages, advises, or administers approximately $1.3 trillion in assets.