SEI Trust Company

Quarterly Update
June 30, 2021

SEI New ways. New answers.®

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

- **Recording of Call with an ERISA Plan Participant Must Be Made Available to that Participant, Says the US Department of Labor**

In a June 14, 2021 information letter[1], the US Department of Labor (DOL) opined that a claimant appealing an adverse benefit determination under a plan covered by the Employee Retirement Income Security Act of 1974, as amended (ERISA), has the right under the statute to request audio recordings of customer service calls made during the claims process.

Many service providers providing services to plan participants and other plan fiduciaries may be recording telephone conversations in accordance with their respective state law requirement, in the ordinary course of their business. Many state laws require consent from both parties to the call in order to record the call, while other state laws do not require such consent. But often ERISA plan service providers, especially those who are discussing matters regarding benefit determinations with plan participants, use call recording to help substantiate the administrative record, especially when necessary to support an adverse benefit determination made against a plan participant's claim. However, not every service provider provides a copy of those call logs and recording to plan participant when requested by a plan participant or his/her counsel after an adverse benefit determination, as those call recordings are not necessarily considered part of the official records of the determination.

Not surprisingly, the US. Department of Labor (DOL) has taken a different view, based upon the reading of the applicable regulations[2], which states that information is relevant to the benefit determination if it:

(i) was relied upon in making the benefit determination; (ii) was submitted, considered, or generated in the course of making the benefit determination, without regard to whether such document, record, or other information was relied upon in making the benefit determination; (iii) demonstrates compliance with the administrative processes and safeguards required pursuant to paragraph (b)(5); or (iv) constitutes a statement of policy or guidance with respect to the plan concerning the denied treatment option or benefit for the claimant's diagnosis, without regard to whether such advice or statement was relied upon in making the benefit determination.

[1] See Information Letter 06-14-2021 available at https://www.dol.gov/agencies/ebsa/about-ebsa/our-activities/resource-center/information-letters/06-14-2021

[2] 29 CFR 2560.503-1(m)(8).

"As subparagraph (ii) states, information is relevant to a claimant's claim if it "was … generated in the course of making the benefit determination," even if it was not "relied upon in making the benefit determination." Consequently, for purposes of subparagraph (ii) it is immaterial whether information was "not created, maintained, or relied upon for claim administration purposes."[3]

Further, the DOL noted that nothing in the regulations support a conclusion that records had to be in paper format, or any specific format for that matter, for the disclosure requirements to apply for purposes of appealing an adverse benefit determination. So, again, not surprisingly, the DOL opined in its informational letter, that it would expect service providers who maintain recordings of telephone calls with plan participants, to provide a copy of the recording or transcript when requested as part of a review of the administrative records following a benefit determination.

As a matter of clarification, the letter is not binding on courts or technically even on the DOL itself. The letter was provided pursuant to ERISA Procedure 76-1, which states: "An information letter issued by the department is informational only and is not binding on the department with respect to any particular factual situation." Although federal courts will sometimes defer to formal agency rules and rulings, they generally will not defer to other expressions of agency opinions.

- **Updates on Regulatory Cybersecurity Initiatives Instituted by both the DOL and the US Securities & Exchange Commission**

By now, most everyone knows that cybersecurity practices are a top priority at most, if not all, state and federal regulators, including both the DOL and the US Securities & Exchange Commission (SEC). Here's a brief update on what is happening at both:

SEC: Recent Enforcement Action

The U.S. Securities and Exchange Commission (SEC) has recently announced its first large civil monetary penalties and a cease-and-desist order against First American Financial Corporation (FAFC) for deficient disclosure controls and procedures related to cybersecurity risks. The action was taking in connection with the New York State Department of Financial Services' (NYSDFS) first-ever charges for violating the NYSDFS' Cybersecurity Regulations.

The case alleged arose as follows: On May 24, 2019, a cybersecurity journalist notified FAFC's investor relations personnel that its web application for sharing document images related to title and escrow transactions had a cybersecurity vulnerability that exposed sensitive personal information from more than 800 million documents from real estate transactions, including bank account numbers, mortgage and tax records, Social Security numbers, wire transactions receipts and drivers' licenses images. After FAFC shut down external access to this web application, the journalist published an article regarding the vulnerability.

Following an investigation on the claim, on June 15, 2021, the SEC announced that it had settled its enforcement action against FAFC with an agreed to cease-and-desist order and a civil monetary penalty of $487,616. The SEC found that FAFC's deficient disclosure controls and procedures related to cybersecurity risks violated Rule 13a-15(a) under the Securities Exchange Act of 1934, as amended (Exchange Act), which requires issuers registered under Section 12 of the Exchange Act to maintain disclosure controls and procedures to ensure the timely and accurate reporting of information as required by the SEC's rules and forms.

The SEC concluded that FAFC senior executives lacked information necessary to evaluate FAFC's cybersecurity responsiveness and the magnitude of the risk from the web application's vulnerability at the time they approved the Form 8-K. Despite being in the business of providing services related to real estate transactions, the SEC determined that FAFC ". . . did not have any disclosure controls and procedures related to cybersecurity, including incidents involving potential breaches of that data."[4] In announcing this settlement, the chief of the SEC Enforcement Division's Cyber Unit warned that "[i]ssuers must ensure that

[3] See Information Letter 06-14-2021.

[4] See *SEC Press Release, SEC Charges Issuer With Cybersecurity Disclosure Controls Failures*, https://www.sec.gov/news/press-release/2021-102

information important to investors is reported up the corporate ladder to those responsible for disclosure."

DOL: New Cybersecurity Guidance and Commencement of Examinations Focusing on Cybersecurity

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 U.S. Government Accountability Office report urging the DOL to issue cybersecurity recommendations, establishes the DOL's minimum expectations for addressing cybersecurity risks.[5] The guidance was issued in three parts. The first part was *Cybersecurity Program Best Practices*, issued for use by plan sponsors. The second part was *On Line Security Tips*, which was directed to plan participants and beneficiaries who access their retirement account information on line. Then finally, the DOL issued *Tips for Hiring a Service Provider with Strong Cybersecurity Practices*, which although directed to plan sponsors, has meaning for plan service providers and third party fiduciaries, since it outlines what plan sponsors and named fiduciaries will be asking plan service providers going forward. Several plans may even ask the plan service provider to confirm that it meets the guidelines of the guidance, without asking for specifics.

Generally, the *Tips* guidance outlines the type of due diligence that a plan sponsor should engage in before hiring a plan fiduciary, especially one that handles sensitive plan level recordkeeping data like plan participant names, addresses, social security numbers and the like. It recommends plan sponsors ask about the service provider's information security standards, practices and policies, ask the service provider how it validates its practices, and what levels of security standards it has met and implemented, evaluate the service provider's track record in the industry, ask about past breaches and remediation efforts and ask about cyber-insurance policies. Further, the DOL recommends that plan sponsors add the following provisions to their contracts with service providers: information reporting, appropriate confidentiality provisions, notification of breaches, compliance with records retention requirements, and confirmation of cybersecurity insurance. Also important is what is not in the *Tips* guidance, which does not specify any specific cybersecurity requirements, like adherence to any specific industry standards, or requires any specific indemnification provisions in any service provider contracts. Like most activities that a plan fiduciary takes on behalf of a plan, the plan sponsor is directed to have prudence oversight of a plan service provider by understanding the specifics of the service provider's cybersecurity standards and the appropriate contractual protections for the plan and its participants.

Much like the Informational Letter outlined above, the guidance is not binding on courts or technically on the DOL itself. However, although the DOL only issued its first cybersecurity guidance in April, it has been reported that several entities have already received DOL examination requests surrounding their cybersecurity practices.[6] It is reported that the examination request list includes the following informational requests:

"*All policies, procedures, or guidelines relating to: Data governance, classification, and disposal, The implementation of access controls and identity management, including any use of multi-factor authentication, The processes for business continuity, disaster recovery, and incident response, The assessment of security risks, Data privacy, 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, Cybersecurity awareness training, and Encryption to protect all sensitive information transmitted, stored, or in transit*

All documents and communications relating to any past cybersecurity incidents

All security risk assessment reports

All security control audit reports, audit files, penetration test reports and supporting documents, and any other third-party cybersecurity analyses

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

[5] See *Cybersecurity* available on the DOL's website at: https://www.dol.gov/agencies/ebsa/key-topics/retirement-benefits/cybersecurity

[6] See *Well that was fast: The Department of Labor commences cybersecurity audit activity* available at https://www.nixonpeabody.com/en/ideas/articles/2021/06/23/dol-cybersecurity-audits

All documents describing any secure system development life cycle (SDLC) program, including penetration testing, code review, and architecture analysis

All documents describing security technical controls, including firewalls, antivirus software, and data backup

All documents and communications from service providers relating to their cybersecurity capabilities and procedures

All documents and communications from service providers regarding policies and procedures for collecting, storing, archiving, deleting, anonymizing, warehousing, and sharing data.

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."[7]

It is not clear as to whom the target of the examinations are, plan sponsors or plan service providers, but those who service plans should take note to ensure that they have appropriate responses in case the DOL comes knocking with the same or similar request lists. The DOL generally has wide latitude to review documents and services related to ERISA covered plans and plan products, and preparedness will be the key to bringing any DOL exam to a timely and successful conclusion.

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 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) is a leading global provider of investment processing, investment management, and investment operations solutions that help corporations, financial institutions, financial advisors, and ultra-high-net-worth families create and manage wealth. As of March 31, 2021, through its subsidiaries and partnerships in which the company has a significant interest, SEI manages, advises or administers approximately $1.3 trillion in hedge, private equity, mutual fund and pooled or separately managed assets, including approximately $399 billion in assets under management and $880 billion in client assets under administration.

[7] Id.