UWMF Retirement Plan Committee

September 9, 2021, 7:00-8:30 AM

Via WebEx: https://uwhealth.webex.com/uwhealth/j.php?MTID=m0b145b0caceebc801a820bb578b53cef

Meeting Number: 262 024 39473 // Password: 090921


**ADVANCE MEETING MATERIALS ARE POSTED FOR REFERENCE. OCCASIONALLY, THE POSTED MATERIALS DO NOT REFLECT CHANGES MADE SHORTLY BEFORE OR DURING COMMITTEE MEETINGS. THE FULL COMMITTEE MINUTES ARE THE OFFICIAL RECORD OF FINAL COMMITTEE ACTION**
# Agenda

<table>
<thead>
<tr>
<th>Time</th>
<th>Item</th>
<th>Speaker(s)</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>7:00 AM</td>
<td>I. Call to Order</td>
<td>Dr. Venkat Rao</td>
<td></td>
</tr>
<tr>
<td>7:00 AM</td>
<td>II. Consent Agenda</td>
<td>Approval</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Meeting Minutes - Open Session</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Physician Retirement Plan Contribution Requests</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Attachment - Physician Retirement Plan Contribution Requests</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>7:05 AM</td>
<td>III. Fidelity Investments</td>
<td>Mr. David Bruce</td>
<td>Report/Discussion</td>
</tr>
<tr>
<td></td>
<td>Fidelity Investments</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Presentation - Fidelity Investments</td>
<td></td>
<td>11</td>
</tr>
<tr>
<td>7:35 AM</td>
<td>IV. RVK Updates</td>
<td>Ms. Jennifer Sandberg, Ms. Elise Willey</td>
<td>Report/Discussion</td>
</tr>
<tr>
<td></td>
<td>2021 RVK Defined Contribution Regulatory &amp; Legislative Overview</td>
<td></td>
<td>22</td>
</tr>
<tr>
<td></td>
<td>Presentation - 2021 RVK Defined Contribution Regulatory &amp; Legislature Overview</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8:30 AM</td>
<td>V. Adjourn</td>
<td></td>
<td>Meeting may adjourn prior to 8:30 AM</td>
</tr>
</tbody>
</table>
Per the Plan Document:

“Assignment of a physician to a particular contribution category is made by ‘the Employer’ [UWMF](through its Retirement Plan Committee or otherwise).”
## Clinical Anesthetist

<table>
<thead>
<tr>
<th>Name</th>
<th>Department</th>
<th>Start Date</th>
<th>PRP % Request</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fitawok (Belay) CAA, Mikiyas</td>
<td>Anesthesiology</td>
<td>8/1/2021</td>
<td>5%</td>
</tr>
<tr>
<td>Lenz CAA, Richard T</td>
<td>Anesthesiology</td>
<td>8/1/2021</td>
<td>20%</td>
</tr>
<tr>
<td>Moses CAA, John T</td>
<td>Anesthesiology</td>
<td>8/1/2021</td>
<td>15%</td>
</tr>
</tbody>
</table>
# UWMF Physicians Retirement Plan
## Contribution Category Requests - New Hires

### Fellows

<table>
<thead>
<tr>
<th>Name</th>
<th>Department</th>
<th>Start Date</th>
<th>PRP % Request</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bailey MD, Erin J</td>
<td>Clinical Instructor</td>
<td>8/1/2021</td>
<td>25%</td>
</tr>
<tr>
<td>Buttigieg MD, Emily</td>
<td>Clinical Instructor</td>
<td>7/26/2021</td>
<td>15%</td>
</tr>
<tr>
<td>Chau MD, Steven Minh</td>
<td>Clinical Instructor</td>
<td>8/1/2021</td>
<td>0%</td>
</tr>
<tr>
<td>Chiu MD, Alexander</td>
<td>Clinical Instructor</td>
<td>8/1/2021</td>
<td>0%</td>
</tr>
<tr>
<td>Danobeitia MD PhD, Juan Sebatian</td>
<td>Clinical Instructor</td>
<td>8/1/2021</td>
<td>5%</td>
</tr>
<tr>
<td>Kuei MD, Michelle</td>
<td>Clinical Instructor</td>
<td>8/1/2021</td>
<td>25%</td>
</tr>
<tr>
<td>LaRocque MD PhD, Joshua</td>
<td>Clinical Instructor</td>
<td>8/1/2021</td>
<td>15%</td>
</tr>
<tr>
<td>Masson MD, Rajeev K</td>
<td>Clinical Instructor</td>
<td>8/1/2021</td>
<td>0%</td>
</tr>
<tr>
<td>Philip MD, Jennifer L</td>
<td>Clinical Instructor</td>
<td>8/1/2021</td>
<td>5%</td>
</tr>
<tr>
<td>Vithayathil MD, Paul J</td>
<td>Clinical Instructor</td>
<td>8/1/2021</td>
<td>25%</td>
</tr>
<tr>
<td>Wong MD, Kristen A</td>
<td>Clinical Instructor</td>
<td>8/1/2021</td>
<td>15%</td>
</tr>
<tr>
<td>Name</td>
<td>Department</td>
<td>Start Date</td>
<td>PRP % Request</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------------------------------</td>
<td>------------</td>
<td>---------------</td>
</tr>
<tr>
<td>Accavitti MD, Michael</td>
<td>Clinical Assistant Professor</td>
<td>7/15/2021</td>
<td>25%</td>
</tr>
<tr>
<td>Biswal MD, Sandip</td>
<td>Visiting Professor</td>
<td>8/9/2021</td>
<td>15%</td>
</tr>
<tr>
<td>Chodara MD, Ann</td>
<td>Assistant Professor (CHS)</td>
<td>8/1/2021</td>
<td>15%</td>
</tr>
<tr>
<td>Daun MD, Mitchell</td>
<td>Clinical Assistant Professor</td>
<td>8/1/2021</td>
<td>5%</td>
</tr>
<tr>
<td>Grzybowski MD, Jeffrey S</td>
<td>Assistant Professor (CHS)</td>
<td>8/9/2021</td>
<td>15%</td>
</tr>
<tr>
<td>Hillerson MD, Dustin</td>
<td>Clinical Assistant Professor</td>
<td>8/1/2021</td>
<td>15%</td>
</tr>
<tr>
<td>Ircink MD, James</td>
<td>Clinical Assistant Professor</td>
<td>8/1/2021</td>
<td>15%</td>
</tr>
<tr>
<td>Kratz MD, Jeremy</td>
<td>Assistant Professor</td>
<td>8/1/2021</td>
<td>0%</td>
</tr>
<tr>
<td>LaSenna MD, Charlotte</td>
<td>Assistant Professor (CHS)</td>
<td>7/28/2021</td>
<td>25%</td>
</tr>
<tr>
<td>Less MD, Kathryn</td>
<td>Clinical Assistant Professor</td>
<td>8/1/2021</td>
<td>25%</td>
</tr>
<tr>
<td>Levinson MD, Justin</td>
<td>Assistant Professor (CHS)</td>
<td>7/27/2021</td>
<td>10%</td>
</tr>
<tr>
<td>Lutz MD, Megan K</td>
<td>Assistant Professor (CHS)</td>
<td>8/1/2021</td>
<td>25%</td>
</tr>
<tr>
<td>Narayan MD, Anand K</td>
<td>Associate Professor (CHS)</td>
<td>8/1/2021</td>
<td>10%</td>
</tr>
<tr>
<td>Pap MD, Andrew</td>
<td>Clinical Assistant Professor</td>
<td>8/1/2021</td>
<td>0%</td>
</tr>
<tr>
<td>Patel MD, Ravi</td>
<td>Clinical Assistant Professor</td>
<td>8/1/2021</td>
<td>25%</td>
</tr>
</tbody>
</table>
## Faculty

<table>
<thead>
<tr>
<th>Name</th>
<th>Department</th>
<th>Start Date</th>
<th>PRP % Request</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rakel MD, David</td>
<td>Professor/Dept Chair</td>
<td>7/12/2021</td>
<td>20%</td>
</tr>
<tr>
<td>Seaborg MD, Kristin</td>
<td>Assistant Professor (CHS)</td>
<td>8/1/2021</td>
<td>15%</td>
</tr>
<tr>
<td>Selkie MD, Ellen M</td>
<td>Assistant Professor</td>
<td>7/15/2021</td>
<td>15%</td>
</tr>
<tr>
<td>Sleeth MD, Carolyn</td>
<td>Clinical Assistant Professor</td>
<td>8/1/2021</td>
<td>15%</td>
</tr>
<tr>
<td>Sobecki-Rausch MD, Janelle</td>
<td>Assistant Professor (CHS)</td>
<td>8/1/2021</td>
<td>10%</td>
</tr>
<tr>
<td>Sun MD, Zhuyi E</td>
<td>Assistant Professor (CHS)</td>
<td>8/1/2021</td>
<td>5%</td>
</tr>
<tr>
<td>Swietlik MD, John F</td>
<td>Clinical Assistant Professor</td>
<td>8/1/2021</td>
<td>15%</td>
</tr>
<tr>
<td>Toia MD, Giuseppe</td>
<td>Assistant Professor</td>
<td>8/1/2021</td>
<td>25%</td>
</tr>
<tr>
<td>Tsuchida MD, Ryan E</td>
<td>Assistant Professor (CHS)</td>
<td>8/1/2021</td>
<td>15%</td>
</tr>
<tr>
<td>Webb MD, Bryn</td>
<td>Associate Professor (CHS)</td>
<td>8/1/2021</td>
<td>15%</td>
</tr>
<tr>
<td>Youssef MD PhD, Amr A</td>
<td>Clinical Assistant Professor</td>
<td>7/26/2021</td>
<td>15%</td>
</tr>
<tr>
<td>Zandieh MD, Ali</td>
<td>Clinical Assistant Professor</td>
<td>8/1/2021</td>
<td>15%</td>
</tr>
<tr>
<td>Zurbriggen MD, Luke</td>
<td>Clinical Assistant Professor</td>
<td>8/1/2021</td>
<td>5%</td>
</tr>
</tbody>
</table>
## Contribution Statistics by Physician Group

<table>
<thead>
<tr>
<th>Group</th>
<th>Total</th>
<th>Contributing 0%</th>
<th>Contributing &gt;0%</th>
<th>% Contributing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clinical Anesthetist</td>
<td>3</td>
<td>0</td>
<td>3</td>
<td>100%</td>
</tr>
<tr>
<td>Fellows</td>
<td>11</td>
<td>3</td>
<td>8</td>
<td>73%</td>
</tr>
<tr>
<td>Part-Time Faculty (0%-49% FTE)</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>100%</td>
</tr>
<tr>
<td>Full-Time Faculty (50%-100% FTE)</td>
<td>26</td>
<td>2</td>
<td>24</td>
<td>92%</td>
</tr>
</tbody>
</table>
## Contribution Statistics by Category

<table>
<thead>
<tr>
<th>Category</th>
<th>Total Number Contributing</th>
<th>Total Percentage Contributing</th>
</tr>
</thead>
<tbody>
<tr>
<td>0%</td>
<td>5</td>
<td>12%</td>
</tr>
<tr>
<td>5%</td>
<td>6</td>
<td>14%</td>
</tr>
<tr>
<td>10%</td>
<td>3</td>
<td>7%</td>
</tr>
<tr>
<td>15%</td>
<td>17</td>
<td>40%</td>
</tr>
<tr>
<td>20%</td>
<td>2</td>
<td>5%</td>
</tr>
<tr>
<td>25%</td>
<td>9</td>
<td>21%</td>
</tr>
</tbody>
</table>
University of Wisconsin Medical Foundation

Service Team Intros & DOL Cyber Security Guidance
UW Health Service Team: Key Roles and Responsibilities

Managing Director – Dave Bruce  
**David.Bruce@fmr.com**  
401-292-7720 (cell – 978-340-0104)

- Responsible for overall client satisfaction
- Manages service team and coordinates service delivery
- Conducts annual business planning and retirement plan reviews
- Communicates corporate events
- Consults on new services and best practices

Communication Consultant – Laura Heck  
**laura.heck@fmr.com**  
401-292-3692

- Collaborates with UW Health to develop and implement communication & education programs
- Reviews Financial Wellness and Total Well-Being opportunities
- Analyzes response rates and campaign data to improve engagement and drive action

Client Service Manager – Kintu Camp  
**Kintu.Camp@fmr.com**  
817-474-6081

- Manages all recordkeeping services and plan operations reconfigurations
- Coordinates all plan level events, facilitates new service rollouts, implements best practices

Client Service Administrator – Mandy Jackson-Leach  
**Mandy.Jackson@fmr.com**  
888-579-7526, option 1, ext. 20650

- Works on day-to-day plan operations and is responsible for supporting your transaction processing needs, such as education and training – PSW and NetBenefits®, participant indicative data, reporting, and statements

5500 Reporting/Preparation- Jeanette Williams  
**Jeanette.Williams@fmr.com**  
866-724-4015 x24273

Non-Discrimination Testing- Jeanette Williams  
**Jeanette.Williams@fmr.com**  
866-724-4015 x24273

Fidelity Workplace Consulting – Ashley Heck  
**Ashley.Heck@fmr.com**  
317-478-5091

- Assists in the estimated coverage and general testing analysis – Projection Testing
Workplace Regional Manager – Bill Hochleutner  Bill.Hochleutner@fmr.com 859-386-4572

- Responsible for managing the retirement planners
- Works with retirement planners to make sure customer satisfaction measures are met
- Partners with Communication Consultant to ensure our planners know what is being communicated more broadly by Fidelity and driving topics in their daily appointments

Retirement Planners –
Bob Intoccia  Bob.Intoccia@fmr.com  630-360-5979  
Sasha Owens  Sasha.Owens@fmr.com  312-405-9579

- Retirement Planners use a needs-based approach designed to help all of your employees engage with the benefits you offer and take steps to improve their financial health
- Focus on employees: Actively saving, May be individuals with more complex financial needs, Saving at all levels, Managing finances on monthly basis
- Helps employees: Save for retirement, Grow & protect investments, Turn savings into income, Make retirement decisions, Reducing debt, Build emergency savings, Save for major purchases, Save for retirement by enrolling the retirement plan, Grow & protect investments, overall retirement readiness

Investment Strategist – Tom Brachowski  thomas.brachowski@fmr.com  312-777-5648

- Dedicated resource to help UW Health and your third-party partners manage your investment oversight responsibilities
- Plan and investment menu benchmarking, participant behavior and rate of return analysis
- Conduit to Fidelity Asset Management as well as investment thought leadership
DIGITAL & CYBER READINESS

Digital contact information & cybersecurity preparedness for your plan participants
Plan sponsors

Designed to assist plan sponsors fiduciaries in their evaluation of the cybersecurity practices of service providers.

Cybersecurity Best Practices

Best practices for recordkeepers and other service providers outlining key elements of a cybersecurity program.

Online Security Tips for Retirement Investors

A series of recommendations for plan participants to prevent fraud and loss of access to a retirement account.
Fidelity’s comprehensive cybersecurity program aligns with the DOL’s guidance on cybersecurity best practices

Comparison of the 12 Best Practices

1. **Have a formal, well documented cybersecurity program.**
   Fidelity maintains a set of 50+ information security policies, standards, and technical implementation guides, which cover areas such as platform security, database security, application security, and other supporting technologies (e.g., corporate and personal firewalls, network security, cryptography, and remote access). Our policies are reviewed annually and tested as part of our ISO 27001 certification audit.

2. **Conduct prudent annual risk assessments.**
   Fidelity conducts thorough risk assessments on an annual basis. As part of this process, potential threats to applications are identified, along with the likelihood and impact to determine the inherent risk. Risk ratings are assigned and any findings are formally reported, tracked, and remediated where appropriate.

3. **Have a reliable annual third-party audit of security controls.**
   Fidelity maintains a comprehensive external audit program. Fidelity earned the ISO 27001 certification in 2011 and is currently a holder of this certification. The certification requires annual on-site audits at Fidelity locations across the United States. The audits include in-depth analyses of 114 separate controls supporting multiple technology platforms.
   
   Fidelity’s Type II / SOC 1 audits provide independent assurance by documenting, examining, and testing a wide array of internal controls and information security practices within our service organizations. An independent third-party accounting firm conducts this audit annually for our product lines and the Fidelity data centers. In addition, the third-party auditor conducts an annual SysTrust (SOC 3) examination. The SOC 3 evaluates Fidelity’s network and data center infrastructure in four categories – security, confidentiality, integrity, and availability. The audit results have been unqualified.
   
   Fidelity has become the first retirement and benefits provider in the U.S. to be certified against the international standard for data privacy, ISO 27701. ISO 27701 complements the ISO 27001 data security certification held for the past 9 years. This milestone in privacy risk management demonstrates Fidelity’s commitment to the disclosure, use, and sharing of Personally Identifiable Information (PII) against internationally recognized best practices.

4. **Clearly define and assign information security roles and responsibilities.**
   Fidelity security governance begins at the top, with an executive commitment to information security and a board-driven cybersecurity program. Fidelity’s cybersecurity program is supported by a Chief Information Security Officer (CISO) and a dedicated staff of 900+ security professionals.

5. **Have strong access control procedures.**
   Fidelity implements a Roles-Based Access Control (RBAC) model, based on Access Appropriate to Role (AATR). In this model, Fidelity associates are assigned to specific, management authorized job roles that limit access to only that which is required to perform their functions. Associate access is reviewed on a periodic basis. In addition, system access is deleted in a timely manner for terminated and transferred employees.
Fidelity’s comprehensive cybersecurity program aligns with the DOL’s guidance on cybersecurity best practices

Comparison of the 12 Best Practices (continued)

6. **Ensure that any data stored in a cloud or managed by a third-party service provider are subject to appropriate security reviews and independent security assessments.**

   We only work with trusted cloud service providers that are capable of maintaining security measures that meet or exceed Fidelity requirements. This includes, but is not limited to, requiring our trusted cloud partners to provide regular third-party audit reports on their controls (e.g., ISO 27001, SOC 2) and technology reviews. Fidelity maintains a Vendor Risk Management Program that requires regular technology and business risk reviews of all vendors, including our cloud providers, process or store client information. Vendors that process or store participant personally identifiable information (PII) have risk reviews conducted on a regular basis. In addition to the evaluation of cloud service providers at the vendor level, Fidelity’s Enterprise Cloud Computing (ECC) team serves as an independent governance and cloud enablement organization that conducts reviews and assessments on all individual services that are used in conjunction with our cloud deployments. If a service is not approved by ECC, it cannot be used by Fidelity business unit development teams. Once a service is approved for usage, ECC develops security guardrails and configuration requirements for that service to ensure cloud resources and data is adequately secured.

7. **Conduct periodic cybersecurity awareness training.**

   Fidelity has a mature information security awareness and training program, including mandatory training, to ensure that all Fidelity associates are aware of and comply with information security policies. The program includes areas such as information security principles, incident response, social engineering, along with the classification and handling of private and proprietary information.

   Fidelity also has a comprehensive phishing education and awareness program. Our strategy centers on educating employees about phishing scams. In addition to detailed postings to our internal and external websites, Fidelity launches multiple phishing email campaigns throughout the year. These campaigns test associates on how to recognize and properly report potential phishing emails.

8. **Implement and manage a secure system development life cycle (SDLC) program.**

   Fidelity’s procedures and development methodologies incorporate security into the system development lifecycle. This includes, but is not limited to, security training of application developers, pre-release assessments (secure code reviews), annual penetration tests of externally facing applications, and regular network vulnerability scans.

9. **Have an effective business resiliency program addressing business continuity, disaster recovery, and incident response.**

   Fidelity has established and maintains an enterprise-level ISO 22301-certified business resiliency program that includes both disaster recovery and business continuity. The program includes business resiliency and disaster recovery planning, testing, and ongoing training. The Fidelity Service Center (FSC) provides 24 hours a day, 7 days a week monitoring of the health of our production applications, infrastructure, network, and hardware. The center operates as an end-to-end IT operations service provider, offering capabilities from proactive monitoring to incident management and resolution. The FSC maintains complete redundancy of services across multiple Fidelity locations and serves as a common point of escalation for technology incidents. The FSC is capable of paging support contacts from all internal Fidelity technical teams as well as third-party providers and has built relationships with each Fidelity business unit in order to understand and support their unique needs.
10. Encrypt sensitive data, stored and in transit.
Fidelity employs a wide range of encryption solutions to meet our security needs. Only recognized, industry standard algorithms and implementations of those algorithms are approved for use. Fidelity encrypts customer data in transit over public networks, PII at rest in recordkeeping systems and databases, portable devices, storage on backup tape, and encryption of removable media devices. All data at rest and in transit is encrypted in the cloud.

11. Implement strong technical controls in accordance with best security practices.
Fidelity maintains a defense-in-depth security architecture that includes preventative, detective, and corrective technical controls. Fidelity’s protected and monitored hosting environment includes 24x7x365 physical security, comprehensive network security controls, and access limited to screened associates in an approved job role. Comprehensive network security controls include firewalls, DDoS, intrusion detection and prevention tools to provide event detection and traffic monitoring, anti-virus, advanced malware, proxy servers, anti-spam, vulnerability scanning, penetration testing, and hardened operating systems, applications and databases.

12. Appropriately respond to any past cybersecurity incidents.
Fidelity has established comprehensive information security incident management processes to include documented and tested cyber incident response playbooks. Fidelity’s Security Operations Center (SOC) receives automated security alerts from various systems. Fidelity has clearly defined escalation and analytical processes in place to identify the root cause, assess the risk exposure, minimize the impact of the threat, and protect business operations. Where appropriate, personnel will preserve the necessary evidence, inform legal authorities, and perform forensic analyses. Our incident response process is ISO 20000 and 27001 certified. Additionally, incident management is covered as part of the annual SOC 1 certification by PricewaterhouseCoopers. Fidelity will notify plan sponsors of a data breach in accordance with regulatory requirements and contractual obligations.
Digital Enablement
As of Q2 2021

<table>
<thead>
<tr>
<th>Digital Enablement</th>
<th>Your Results</th>
<th>Industry Peers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow electronic delivery</td>
<td>84%</td>
<td>75%</td>
</tr>
<tr>
<td>Have an email on file</td>
<td>100%</td>
<td>94%</td>
</tr>
<tr>
<td>Employee provided email</td>
<td>93%</td>
<td>87%</td>
</tr>
<tr>
<td>Have a mobile phone on file</td>
<td>86%</td>
<td>80%</td>
</tr>
<tr>
<td>Two factor authentic use</td>
<td>4%</td>
<td>3%</td>
</tr>
<tr>
<td>Enrolled in MyVoice℠</td>
<td>25%</td>
<td>32%</td>
</tr>
</tbody>
</table>

Consider these steps

- Provide Fidelity with contact information for all employees so they can receive alerts about account activity.
- Encourage employees to provide digital contact information, enroll in eDelivery and monitor their accounts regularly.
- Encourage employees to enroll in MyVoice℠ biometric security when calling Fidelity.
Digital enablement and engagement

Overview

Digital Contact Information (DCI) Enablement

77%
Are fully digital ready and meet all 4 criteria1
68% Peer Rate

- Allow electronic delivery: 84% (75% peer rate)
- Have an email on file: 100% (94% peer rate)
- Have a mobile phone on file: 86% (80% peer rate)
- Registered on NetBenefits®: 94% (83% peer rate)

Digital Engagement

- Online Visits: 5.4K Interacted online with Fidelity
- Visit Duration: 3:26 Average time spent per visit online
- Device Type: 55% Desktop, 41% Mobile, 4% Tablet
- Transactions: 2,154 Unique visitors online, who completed at least one online transaction

---

1. "Participants that are fully digital ready" represents employees who have an email on file, have registered accounts on NetBenefits, have a mobile phone number on file and have given permission for electronic delivery. Fidelity record kept data as of 6/30/2021 for active participants with a balance. Excludes terminated and zero balance participants. Also excludes forfeiture and alternate payee accounts.

706485.20.0. INSTITUTIONAL PLAN SPONSOR USE ONLY
Helping employees secure their accounts
Based on all active employees with a balance

Registered
- Logged in and established password on NetBenefits®
  - 94%
  - 0.6% unregistered, no contact info
  - 4.9% unregistered, with contact info

Monitoring
- Logged into account in last 90 days
  - 53%
  - 59.8% among registered employees

Optimizing security features
- Eligible for two-factor authentication at login
  - 91%
  - 3.8% currently enrolled
- Enrolled in MyVoice℠ voice biometric in phone channel
  - 25%
  - 25.3% acceptance rate
- Eligible to receive real-time alerts
  - 99%
  - 86.5% receive SMS alerts

Top 5 ways to protect your employees from cyber fraud

1. Encourage employees to create a unique username and password on NetBenefits® and provide digital contact information.
2. Encourage employees to enroll in eDelivery and monitor their accounts regularly.
3. Enroll in two-factor authentication at login.
4. Encourage employees to enroll in MyVoice℠ biometric security when calling Fidelity.
5. Provide Fidelity with contact information for all employees so they can receive alerts about account activity.

Fidelity record kept data as of 6/30/2021 for active participants with a balance. Excludes terminated and zero balance participants. Also excludes forfeiture and alternate payee accounts.

706485.20.0. INSTITUTIONAL PLAN SPONSOR USE ONLY
Overview

The goal of the 2021 RVK Defined Contribution Regulatory & Legislative Overview is to provide plan fiduciaries with an update on recent rules, regulations, legislation, and litigation that have impacted or have potential to impact defined contribution (DC) plan sponsors and participants. Despite the ongoing impacts of the COVID-19 pandemic, the past twelve months have seen updates on a number of issues impacting DC plans.

Even before the late 2019 passage of the Setting Every Community Up for Retirement Enhancement Act (SECURE Act), members of the Congress and their staffs were already working on a new round of retirement reform legislation—which has proven to be a rare area of bipartisan agreement in the legislature. Momentum has been gathering on the next round of reforms, a collection of provisions in different areas intended to enhance retirement savings, which have been colloquially named “SECURE 2.0” after the 2019 bill. Key provisions in the latest draft of the bill include mandating auto-enrollment for new DC plans, increasing catch-up contributions, further changes to the age requirements for required minimum distributions, student loan repayment matching, and allowing 403(b) plans to invest in collective investment trusts (“CITs”). At this time, the timeline for SECURE 2.0 to advance is unclear due to competing priorities in Congress, but hope still remains for passage in 2021.

The election of President Joe Biden in November 2020 brought a significant shift to the leadership at the Department of Labor (“DOL”) that will likely affect how the Department approaches key retirement issues, such as the ability for plan sponsors to invest with managers that incorporate environmental, social, and governance (“ESG”) factors and the standards that investment advice fiduciaries must following when working with participants under the Employee Retirement Income Security Act of 1974 (“ERISA”). In recent months, the DOL also released long-awaited guidance on retirement plan cybersecurity and missing participants.

The pandemic did not stem the flow of retirement plan-related litigation, as claims were initiated in 2020 at a record pace. ERISA litigation continues to be driven by familiar themes: breach of fiduciary duty due to excessive fees, multiple vendors, not using lowest-fee share class, active vs. passive offerings, underperforming funds—with cybersecurity and fraud protection emerging as new areas of concern. While litigation used to be a concern primarily for the largest plan sponsors, 2020 continued a trend of ever-smaller plan sponsors being affected. The US Supreme Court is again expected to wade into these retirement plan issues in its upcoming term as it takes on a case against Northwestern University.
Legislative Overview

Although regulators are still providing guidance related to 2019’s SECURE Act, members of Congress and their staffs are already looking to pass the next round of retirement reform legislation.

SECURE Act 2.0 – Potential Legislation

Securing a Strong Retirement Act (HR 2954), known colloquially as “SECURE 2.0”, reflects the next stage of legislation aimed at enhancing retirement regulations. Originally introduced in October 2020, SECURE 2.0 is a bipartisan bill that builds on the SECURE Act (“SECURE 1.0”) by clarifying some items from SECURE 1.0, as well as adding in a variety of retirement reform provisions, including some originally proposed in other bills, such as the recently reintroduced Retirement Security and Savings Act (known as the “Portman-Cardin” bill).

Fundamentally, SECURE 2.0 seeks to increase savings and support retirement income provisions, as well as administrative improvements. The bill includes provisions on a myriad of topics, including contributions, distributions, matching contributions for student loan repayments, reporting disclosures, tax credits for small employers, 403(b) plan updates, and additional administrative correction flexibility.

The bill was approved unanimously in the House Ways and Means Committee on May 5, 2021. It also has received strong bipartisan support in the Education and Labor Committee. In the Senate, the bipartisan Portman-Cardin bill includes many similar provisions, indicating at least partial support for SECURE 2.0 in that chamber. It is expected that the Senate Finance Committee will hold a hearing on Portman-Cardin / SECURE 2.0, and it is expected that negotiations will take place to work out remaining differences between the Senate and House bills. However, SECURE 2.0 will likely not proceed to a floor vote in either chamber until after legislators deal with other priorities, such as infrastructure and the budget. As such, it is unclear whether SECURE 2.0 will pass in 2021, despite its broad bipartisan support. In order to facilitate passage, it is possible that the bill could be attached to a larger piece of must-pass legislation, similar to process that ultimately led to the passage of the SECURE Act. If the bill does not pass in the current legislative session, many of the provisions discussed below likely will continue to re-emerge in proposed legislation until a retirement reform bill is signed into law. Plan sponsors should remain aware of the prospect for additional retirement reform legislation and be prepared to make potential changes to their plans.

A summary of key provisions from the bill applicable to DC plan sponsors is provided below:

---

### Updates Relating to Eligibility and Contributions

<table>
<thead>
<tr>
<th>Provision</th>
<th>Description</th>
<th>Expected Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Required Auto-Enrollment Expansion for New Plans</td>
<td>Effective 2023, new 401(k) and 403(b) plans would be required to auto-enroll participants at a default rate between 3% and 10% with auto-escalation at a rate of 1% annually, up to at least 10%, but no more than 15%. The provision would raise the auto-escalation cap to 15% for safe harbor plans and to 10% for non-safe-harbor plans before 2025 and 15% after 2025. The language excludes governmental plans, church plans, employers with 10 or less employees, SIMPLE 401(k) Plans, and new employers with less than 3 years of operation. Plans forming MEPS are not allowed to grandfather in employers.</td>
<td>Reflective of widespread low levels of participant deferrals, the provision encourages increased participant savings and demonstrates increased recognition by policy-makers of the value of auto-features for encouraging retirement savings.</td>
</tr>
<tr>
<td>Allows Small Contribution Incentives</td>
<td>401(k) and 403(b) plan participants would be allowed to receive de minimis financial incentives (such as a gift card) for contributing to the plan. (With the exception of matching contributions, this is currently prohibited by the IRS Tax Code and ERISA under prohibited transaction rules.)</td>
<td>Relies on principles of behavioral economics to encourage participant retirement savings.</td>
</tr>
<tr>
<td>Increasing Catch-up Contribution Limits</td>
<td>Effective 2023, non-SIMPLE 401(k) plan participants age 62-64 would be allowed to contribute the lesser of $10,000 indexed for inflation, or the level of the participant’s compensation reduced by other elective deferrals, an increase from the current 2021 maximum of $6,500. (A similar provision would also apply to SIMPLE plan participants.)</td>
<td>The provision targets participants who have under contributed, to support participants who attempt to close the gap between retirement savings and retirement needs.</td>
</tr>
<tr>
<td>Roth Expansion</td>
<td><strong>Required Roth Catch-up Contributions:</strong> Effective 2022, 401(a) qualified plan, 403(b), and governmental 457(b) plans that allow catch-up contributions must designate them as Roth contributions.</td>
<td>These provisions demonstrate policymakers’ willingness to use Roth as a near-term revenue source.</td>
</tr>
</tbody>
</table>


| **Roth Employer Contributions:** | Effective at enactment, 401(a) qualified plans, 403(b), and governmental 457(b) plan employers may permit employees to have matching contributions designated as Roth and included in income. |
| **Removed Governmental 457(b) Plan First Day of the Month Deferral Election Requirement** | Post enactment, the provision removes the requirement that participants can only revise their deferral election before the first day of the month in which compensation is paid. The removal of this provisions aligns with other plan types, allowing participants to change their deferral election at any time before compensation is paid to the participant. Removes unnecessary complexity and administrative burdens to governmental 457(b) participants. |
| **Student Loan Repayment Matching** | Effective 2022, 401(k), 403(b), SIMPLE IRAs, and 457(b) plans may allow employer matching contributions for qualified student loan payments. ADP testing may be applied separately to employees receiving matching contributions on student loans. Building on the Abbott Labs private letter ruling, the provision provides a formal path for plan sponsors, recognizing the burden of student loan debt as a hurdle to saving for retirement. |
| **Long-term part-time worker coverage** | SECURE 1.0 required plans to allow long-term part-time employees to contribute to a plan if the employee had worked for at least 500 hours per year for at least three consecutive years and met the minimum age requirement. SECURE 2.0 would reduce the 3-year requirement to 2 years, effective retroactively for plan years the SECURE Act was active. The provision also clarifies that service prior to 2021 is disregarded for vesting of employer contributions. Allows more part-time workers access sooner to a retirement plan to encourage saving for retirement. |

## Updates Relating to Required Minimum Distributions

<table>
<thead>
<tr>
<th>Provision</th>
<th>Description</th>
<th>Expected Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Increased RMD Age</td>
<td>Effective 2022, the provision increases the minimum distribution age from 72 (the age to which it was raised from 70.5 in the SECURE 1.0 Act) to age 73 in 2022, age 74 in 2029, and age 75 in 2032</td>
<td>Delayed RMDs give participants greater flexibility regarding when to begin to draw down their DC plan assets and addresses participant longevity risk as the population lives longer.</td>
</tr>
<tr>
<td>Removed RMD barriers for Life Annuities</td>
<td>Currently, there are limits on the structure of annuity payments in DC plans, including preventing annuities from providing payments that increase over time that don’t meet an actuarial test. Effective at enactment, the provision would provide more flexibility for new types of annuity structures.</td>
<td>Encourages a broader range of lifetime income offerings by removing barriers to annuities.⁶</td>
</tr>
<tr>
<td>RMD Excise Tax Reduction</td>
<td>Effective 2022, the excise tax for failure to take RMDs would be reduced from 50% of the remaining amount of the RMD to 25%. Additionally, if a participant corrects the error within 2 years, the excise tax is reduced to 10%.⁷</td>
<td>Allows participants an opportunity to correct RMD errors and reduces burdens on participants who make mistakes.</td>
</tr>
</tbody>
</table>

⁶ Manganaro, *House Education and Labor Committee Debates SECURE 2.0.*
⁷ Dold, *Comparison of Provisions in SECURE 2.0 and Cardin-Portman.*
**Updates Relating to Withdrawals**

<table>
<thead>
<tr>
<th>Provision</th>
<th>Description</th>
<th>Expected Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardship Distribution Self-Certification</td>
<td>Effective 2022, a participant in a 401(k) plan or 403(b) plan can self-certify that they had a qualifying event that would meet the conditions for a deemed hardship withdrawal. Additionally, plans may rely on participants to certify that the distribution is not above the financial need. (A similar provision applies for governmental 457(b) plan unforeseeable emergency distributions.)</td>
<td>Streamlines the hardship documentation process, making it faster and easier for participants experiencing a hardship to gain access to their money.</td>
</tr>
<tr>
<td>Remove Penalty for Domestic Abuse Cases</td>
<td>Effective at enactment, participants in 401(k), 403(b), and governmental 457(b) plans who have experienced domestic abuse can take an early withdrawal penalty-free up to the lesser of $10,000 or 50% of the participant’s account, and later recontribute that amount back to the plan.</td>
<td>Streamlines the hardship documentation process, making it faster and easier for participants experiencing a hardship to gain access to their money.</td>
</tr>
<tr>
<td>Qualified Longevity Annuity Contracts (“QLACs”) Changes</td>
<td>Effective after enactment, removes the current limit that the QLAC premium payment must be less than 25% of the participant’s account balance. Retroactive to contracts purchased after July 2, 2014, clarifies that a divorce occurring between the purchase of the QLAC and its first payment would not affect the permissibility of the joint and survivor benefits under the contract, and provides a “short free look period” is permitted within up to 90 days of purchase where a participant may rescind the annuity contract.</td>
<td>By reducing these barriers, QLACs can help provide longevity protection to participants.(^8)</td>
</tr>
</tbody>
</table>

---

\(^8\) Manganaro, *House Education and Labor Committee Debates SECURE 2.0*. 
Qualified Birth or Adoption Distribution Repayment

The existing legislation in the SECURE Act did not set a time frame for recontribution of qualified birth or adoption distributions. This provision would align repayment with other disaster relief provisions and require repayment within three years in order to qualify as a rollover contribution, effective retroactively to the SECURE Act passage date, at the bill’s enactment.

<table>
<thead>
<tr>
<th>Provision</th>
<th>Description</th>
<th>Expected Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Qualified Birth or Adoption Distribution Repayment</td>
<td>The existing legislation in the SECURE Act did not set a time frame for recontribution of qualified birth or adoption distributions. This provision would align repayment with other disaster relief provisions and require repayment within three years in order to qualify as a rollover contribution, effective retroactively to the SECURE Act passage date, at the bill’s enactment.</td>
<td>Reduces taxes for distributions to first responders with a disability.</td>
</tr>
<tr>
<td>Disability Exclusions</td>
<td>Effective 2027, disability-related distributions for first responder participants in 401(a), 403(a), governmental 457(b), or 403(b) plans payments are excluded from gross income at retirement age up to the annual excludable limit. This is currently included in taxable income.</td>
<td>Reduces taxes for distributions to first responders with a disability.</td>
</tr>
<tr>
<td>Firefighter Exception</td>
<td>Effective 2022, allows private sector firefighters to take distributions from a qualified retirement plan or a 403(b) plan at age 50, as currently allowed for “qualified public safety employees,” without a 10% early withdrawal penalty.</td>
<td>Removes administrative differences between public and private firefighters.</td>
</tr>
</tbody>
</table>

Investment Updates

<table>
<thead>
<tr>
<th>Provision</th>
<th>Description</th>
<th>Expected Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset allocation fund benchmarks</td>
<td>The provision directs the Secretary of Labor to modify the existing regulation within 6 months of enactment to allow plan sponsors to benchmark mixed asset investment options against a blended benchmark comprised of broad market indices.</td>
<td>Encourages more relevant benchmarks for Target Date Funds.</td>
</tr>
<tr>
<td>ETFs in Insurance Products</td>
<td>Current legislation prevents ETFs from being used by individual variable annuities, as the legislation was written before ETFs existed. This provision removes the regulatory restrictions to offer ETFs in insurance products.</td>
<td>Aims to remove restrictions around annuities to allow for broader product features and potentially increased usage in retirement income solutions.</td>
</tr>
</tbody>
</table>
# Reporting & Disclosure Updates

<table>
<thead>
<tr>
<th>Provision</th>
<th>Description</th>
<th>Expected Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paper Statements</td>
<td>Effective 2023, plan administrators must provide DC participants a paper statement once a year, except where plans allow employees to opt into e-delivery or for plans that use the 2002 safe harbor. Additionally, the Secretary of Labor is directed to update e-delivery rules to include participant protections by the end of 2021.</td>
<td>Provides a potential limitation on industry movement toward e-delivery of participant statements.</td>
</tr>
<tr>
<td>Minimized Communication with Unenrolled Participants</td>
<td>Effective 2022, plan sponsors would only have to notify unenrolled participants annually, rather than the numerous existing communications required under current provisions.</td>
<td>Simplifies plan administration.</td>
</tr>
<tr>
<td>“Lost &amp; Found” Reporting</td>
<td>The Secretaries of Treasury, Labor, and Commerce are directed to create an online “Lost and Found” searchable database that the Pension Benefit Guaranty Corporation (“PBGC”) would maintain for missing, lost or non-responsive participants and beneficiaries of tax-qualified DC plans as well as defined benefit plans. Additionally, the mandatory cash-out provision is increased to $6,000 from $5,000.</td>
<td>Aims to help plans find lost, missing, or non-responsive participants receive the full benefit of accumulated retirement savings; however, the provision imposes additional reporting requirements on plan sponsors.</td>
</tr>
<tr>
<td>Report to Congress</td>
<td>The Secretaries of Treasury and Labor and Director of the Pension Benefit Guaranty Corporation are instructed to review and report to Congress on disclosure and reporting requirements and potential areas for simplification, consolidation, and standardization.</td>
<td>Indicates a desire by legislators to find additional ways to simplify plan reporting and disclosures.</td>
</tr>
</tbody>
</table>
### 403(b) Changes

<table>
<thead>
<tr>
<th>Provision</th>
<th>Description</th>
<th>Expected Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>CITs in 403(b) Plans</td>
<td>Effective 2022, 403(b) plans with custodial accounts can invest in collective investment trusts (“CITs”). Previously, 403(b) plans could only invest in mutual funds and annuities.</td>
<td>These provisions align provisions across DC plans to allow 403(b) plan participants access to similar high-quality and potentially lower-cost investment options and reduce administrative differences from other plan types.</td>
</tr>
<tr>
<td>PEPs and MEPs Expansion</td>
<td>Effective 2022, 403(b) plans can be created as a Multiple Employer Plan or Pooled Employer Plan. 403(b) plans were not included in SECURE 1.0.</td>
<td></td>
</tr>
<tr>
<td>Hardship Withdrawal Rules</td>
<td>Effective 2022, 403(b) plans may distribute qualified matching contributions and earnings on any of these contributions including elective deferral sources on hardship withdrawals.</td>
<td></td>
</tr>
</tbody>
</table>
Regulatory Overview

With the new Administration came leadership changes at the DOL. Boston Mayor Marty Walsh was selected by President Biden to be the new Secretary of Labor. His nomination was approved by the Senate in March 2021. In late July 2021, President Biden nominated Lisa M. Gomez as Assistant Secretary for Employee Benefits, who will oversee the Employee Benefits Security Administration, which has primary responsibility for retirement plans. Ms. Gomez is currently a partner at the law firm Cohen, Weiss, and Simon LLP and has represented various retirement and health and welfare plans during her career in employee benefits law.

Despite the leadership changes, the DOL has already been quite active in promulgating guidance affecting retirement plans. Several key pieces of DOL guidance are discussed on the following pages.

DOL Cybersecurity Guidance

In April 2021, the DOL released long-awaited cybersecurity guidance for plan sponsors, plan fiduciaries, recordkeepers, and participants. In recent years, cyber-attacks against DC plans (as well as other financial institutions) have grown more common, and cybersecurity is seen as an emerging area of DC plan-related litigation. The release marked the first time that the DOL has issued cybersecurity guidance related to retirement plans. The guidance is intended for ERISA plan sponsors and fiduciaries (including sponsors of health and welfare plans), as well as recordkeepers, but it is broadly applicable to all DC plans and participants. There are three pieces to the guidance:

- **Tips for Hiring a Service Provider**
  This document lays out the DOL’s thoughts on how a fiduciary can prudently select and contract with a service provider with good cybersecurity practices, and it states that “plan sponsors should use service providers that follow strong cybersecurity practices.” The “tips” provided by the DOL are:
  - Asking about a provider’s information security standards, practices and policies, and audit results
  - Asking how a service provider validates its practices
  - Evaluating the service provider’s industry track record, such as security incidents and legal proceedings
  - Asking questions regarding prior security breaches, and remediation if any have occurred
  - Determining if the service provider has insurance covering cybersecurity and identity theft breaches

---


Enabling a service provider contract requires ongoing compliance with cybersecurity standards and working to include terms to enhance cybersecurity protection for the plan.

**RVK Comments:** Prior to the DOL's guidance, RVK already asked a range of cybersecurity and data protection questions as part of our recordkeeper and custody due diligence and evaluations. RVK reviewed our standard scope items and technical questions and found they generally met, and in some ways exceeded, the tips provided by the DOL. We have made some additional enhancements to ensure alignment with the DOL’s process and stand ready to assist plan sponsors with their service provider evaluations in concert with appropriate internal and external stakeholders.

- **Cybersecurity Program Best Practices**\(^\text{12}\): In this document, the DOL states “Responsible plan fiduciaries have an obligation to ensure proper mitigation of cybersecurity risks.” The DOL then lays out best practices for recordkeepers and other service providers to follow. There are twelve focus areas stated, including having a formal, well documented cybersecurity program, annual risk assessments and audits, strong access control procedures, a business resiliency program, data encryption, and a responsive approach to breaches.

**RVK Comments:** The DOL’s guidance, which was created in consultation with industry groups such as the SPARK Institute, provides a clear framework for recordkeepers and other service providers to follow in order to provide a reasonable cybersecurity and data protection framework to plans.\(^\text{13}\) Given this industry’s focus and involvement, recordkeepers have produced working papers and other documentation to demonstrate how they meet, and in some cases exceed, the DOL’s guidance.

- **Online Security Tips**\(^\text{14}\): The online security tips document is oriented towards plan participants and is intended to provide a summary of best practices for an individual to secure their own retirement account. The best practices include items such as registering an online account and creating strong and unique passwords, using multi-factor authentication, keeping contact information current, and avoiding phishing attacks.

**RVK Comments:** The DOL’s tips for participants represent a recognition by the DOL that participants themselves play an important role in keeping data safe. Plan sponsors should be aware of this guidance and should actively encourage their participants to follow cybersecurity best practices for their retirement accounts, potentially by sharing the DOL guidance or recordkeeper-generated tips with participants.\(^\text{15}\) We would also encourage all readers to review the tips, regardless of their role working with DC plans, as the tips are


\(^{15}\) Hadley and McMahon, *DOL Issues Cybersecurity Guidance for Retirement Plans*. 
generally good best practices for personal and professional accounts that contain financial or other personal data.

One best practice of note is for participants to register, setup, and monitor their online accounts. Recordkeepers have cited online account setup as a particular vulnerability for retirement plans since some retirement-related best practices (such as auto-enrollment and encouraging participants to avoid frequently checking their accounts and making rash decisions in times of market stress) can result in participants being less likely to notice unusual account activity associated with potential cyber threats. Plan sponsors should be aware that while the “set it and forget it” nature of auto-enrollment and target date funds (TDFs) are important for helping participants build retirement savings, it is important to ensure that participants are adequately protecting their accounts.

It is important to note that the DOL’s guidance is structured as “tips” and “best practices” and does not outline or provide a safe harbor, nor does it address whether plan data should be considered a “plan asset” (which has been the subject of recent litigation). However, the DOL does generally assert that protecting plan accounts is part of a plan sponsor’s fiduciary obligation under existing ERISA regulations. It is expected that the DOL will be active in its audit and enforcement actions related to DC plan cybersecurity as a result of this guidance, which could lead to additional guidance and/or precedential decisions in the future.

Overall, the new guidance represents the DOL’s first attempt at outlining expectations for cybersecurity related to DC retirement plans and provides helpful information to plan sponsors, recordkeepers, and participants. Given the importance of this issue and emphasis from the DOL, DC plan sponsors may want to consider involving internal or external cybersecurity resources in their Committee, as well as reviewing existing service provider contracts and establishing a process for ongoing cybersecurity due diligence. RVK looks forward to continuing to support our DC clients as they continue to work with their service providers to keep participant accounts safe.

**DOL Missing Participants Guidance**

On January 12, 2021, the DOL released three pieces to help provide guidance and best practices for retirement plan fiduciaries related to missing or nonresponsive participants. In recent years missing participants have been a focus of DOL investigations. The recent guidance, which focuses on “red flags” and best practices for plan sponsors, does not necessarily establish rules or enforceable laws for plan fiduciaries, but does provide a more clear understanding of the DOL’s position on the issue. Prior to the most recent guidance, the last guidance was issued in 2014.

---

19 Blachman et al., *A Step Towards Minimum Expectations.*
focusing on missing participants and beneficiaries under a terminated defined contribution plan.\textsuperscript{22} This new guidance is intended to help plan sponsors refine and enhance their current processes for missing participants. The following three pieces of guidance are included:

1. “Best Practices for Pensions Plans” describes the best practices and red flags for fiduciaries of retirement plans, including defined benefit and defined contribution plans, to help reduce missing participant issues and ensure that participants receive their promised benefits when they reach retirement age. Red flags cited by the DOL included items such as more than a small number of missing or nonresponsive participants; terminated/vested and retirement age participants who have not started receiving benefits; missing, inaccurate, or incomplete contact information; and, a lack of policies for handling returned mail or uncashed checks.\textsuperscript{23}

The DOL separates their best practices for both defined benefit and defined contribution plans into four categories, each with a number of items: 1) Maintaining accurate census information for the plan’s participant population; 2) Implementing effective communication strategies; 3) Conducting missing participant searches; and 4) Documenting procedures and actions. The recommendations are generally viewed as prudent and sensible, but plan sponsors should be aware that some may not be feasible depending on the plan’s size and type.\textsuperscript{24} However, the DOL states that “not every practice is necessarily appropriate for every plan” and “plan fiduciaries should consider what practices will yield the best results in a cost-effective manner”.\textsuperscript{25}

2. “Compliance Assistance Release 2021-01” is an internal DOL memo that explains the DOL’s goals and processes in missing participant audits under the Terminated Vested Participant Project (TVPP) published to facilitate voluntary compliance efforts by plan fiduciaries.\textsuperscript{26} The TVPP audit program focuses on identifying defined benefit plans with signs that there may be significant issues in identifying missing participants or beneficiaries and paying benefits at normal retirement age or when required minimum distributions (RMDs) are set to start. This guidance serves as reminder to fiduciaries to review the plan data and procedures should the plan face a TVPP investigation.

3. “Field Assistance Bulletin 2021-01” creates a temporary non-enforcement policy allowing plan fiduciaries that terminate defined contribution plans to use the Pension Benefit Guaranty Corporation’s (PBGC) expanded Missing Participants Program. The Program allows plan fiduciaries of defined contribution plans to transfer remaining accounts balances to the PBGC rather than to an IRA provider or state escheatment program. This is a temporary guidance to

\textsuperscript{23} Kreps et al., \textit{DOL Issues Missing Participants Guidance}.
\textsuperscript{24} Seyfarth. \textit{Missing Participant Guidance Trifecta}.
\textsuperscript{25} US DOL, EBSA, \textit{Missing Participant Guidance}.
help plan fiduciaries meet their responsibilities to distribute account balances after plan termination and will only remain in place until further guidance is released by the DOL.

Overall, the three new pieces provide more clarity regarding the DOL’s position on best practices for plan sponsors dealing with missing participants. Plan sponsors are encouraged to work with their recordkeepers and legal counsel to review existing missing participant-related practices and procedures to determine if any modification should be considered to align with the new guidance.

**DOL Investment Advice PTE 2020-02**

On December 15, 2020, the DOL finalized a new Prohibited Transaction Exemption (“PTE 2020-02”), which allows investment advice fiduciaries to receive compensation while engaging in activities that might otherwise violate the prohibited transaction prohibitions of ERISA and the Internal Revenue Code (“Code”), if a series of requirements are met. PTE 2020-02 also provides a revised interpretation of the “Five-Part Test” for determining who is an investment advice fiduciary under ERISA. The rule package is intended to replace the 2016 Fiduciary Rule and Best Interest Contract (“BIC”) exemption, which were vacated by the 5th Circuit Court of Appeals in 2018.

Since PTE 2020-02 was not scheduled to take effect until after the inauguration, observers generally expected the implementation to be delayed by the new Administration. However, in February 2021, the DOL announced that the rule would go into effect as scheduled on February 16, 2021. The Department also announced that a temporary non-enforcement policy, whereby the DOL would not pursue claims against investment advice fiduciaries attempting in good faith to comply with the 2016 Fiduciary Rule, would end in December 2021.27 In April 2021, the DOL published an FAQ about PTE 2020-0228 as well as a guide for individual investors on how to choose an advice provider.29 In the FAQ, the DOL stated its intention to take further actions regarding investment advice—signaling that it does not consider this to be a settled issue.

Under the 1975 Five-Part Test for determining fiduciary status, to be considered as giving “investment advice,” a financial institution or investment professional that is not otherwise a fiduciary must:

1. render advice...as to the value of securities or other property, or make recommendations as to the advisability of investing in, purchasing, or selling securities or other property
2. on a regular basis
3. pursuant to a mutual agreement, arrangement, or understanding with the Plan, Plan fiduciary or IRA owner that

---


iv. the advice will serve as a primary basis for investment decisions with respect to Plan or IRA assets, and that
v. the advice will be individualized based on the particular needs of the Plan or IRA.  

Any individual or organization that meets the test and receives direct or indirect compensation is considered a fiduciary under ERISA and the Code.

In the preamble to the final PTE 2020-02 (which is not formal regulatory language), the DOL provided commentary on its interpretation of the Five-Part Test that broadens the range of actions that could lead to the determination that a provider is acting as a fiduciary. Most notably, the DOL stated that rollover recommendations are generally investment advice, especially if advice has been given for other accounts or if advice is expected to be given following the rollover—specifically stating that a 2005 DOL Advisory Option (known as the “Deseret Opinion”) no longer reflected its understanding of fiduciary status regarding rollovers. The FAQ expanded upon the language in the preamble and provided a broader spectrum of scenarios where the DOL considers rollover recommendations to be fiduciary investment advice.

Since a person who is a fiduciary (including an investment advice fiduciary per the Five-Part Test above) is subject to ERISA’s prohibited transaction rules, which generally prevent the fiduciary from engaging in certain conflicted transactions—especially principal transactions—investment advice fiduciaries are generally reliant on a prohibited transaction exemption to receive compensation. PTE 2020-02 is intended to provide relief for investment advice fiduciaries to receive compensation that would otherwise be considered the result of a prohibited transaction or “conflicted” as long as certain conditions are met, similar to the goal of the BIC exemption.

An investment provider can meet the requirements of PTE 2020-02 by:

- Adhering to the “Impartial Conduct Standards”, which include a best interest standard, a reasonable compensation standard, a best execution standard, and a no materially misleading statements standard
- Providing various disclosures, including a written acknowledgement of fiduciary status and documentation for any rollover recommendations
- Maintaining policies and procedures to ensure adherence to the Impartial Conduct Standards and mitigate conflicts of interest
- Conducting an annual retrospective review regarding compliance that is reviewed and signed off on by a senior executive of the provider
- Maintaining appropriate records regarding compliance that may be requested by the DOL and the Treasury Department

---

30 US DOL EBSA, *New Fiduciary Advice Exemption.*
33 Kaleda et al., *DOL Interprets Five-Part Investment Advice Test.*
In a change from the proposed rule, the DOL provided a mechanism for financial institutions to self-correct violations of the exemption’s rules.

PTE 2020-02 is in many ways similar to the DOL’s 2016 Fiduciary Rule and BIC exemption, which were widely considered to provide strong protections to investors. One significant difference between the two rules is in the definition of the “best interest” standard; the BIC exemption had stated that recommendations must be made “without regards to” the interests of the advisor, while PTE 2020-02 states that advice must not place the advisor’s interest “ahead of the interests” of the investor, or “subordinate” the interests of the investor. In the preamble, the DOL argued that the PTE 2020-02 definition was a “true” fiduciary standard and consistent with previous guidance, although this is likely to be an area examined by the new Administration. 34

It remains to be seen whether PTE 2020-02 and the reinterpretation of the Five-Part Test will provide appropriate protections to investors, although, as noted earlier, the DOL is expected to continue to examine advice and fiduciary standards in the coming months. RVK continues to closely monitor the situation and will provide further updates as warranted. RVK is also waiting to see how PTE 2020-02 will be used, if at all, by recordkeepers and other providers of advice to DC plan participants. As service providers potentially look to incorporate the new regulations, or possibly adopt alternative service models, plan sponsors should maintain awareness of any advice services being provided to their participants to ensure that they remain appropriate.

DOL & ESG Investing

On March 10, 2021, the Department of Labor (“DOL”) announced that it will not enforce two rules finalized by the previous administration titled: Financial Factors in Selecting Plan Investments (“ESG Rule”) and Fiduciary Duties Regarding Proxy Voting and Shareholder Rights (“Proxy Voting Rule”). Both rules instructed a fiduciary to act solely based on pecuniary or financial factors and were widely seen as discouraging plan sponsors of retirement plans subject to ERISA from implementing investment options that incorporated Environmental, Social, and Governance (“ESG”) factors into their investment processes.

The DOL cited two reasons for non-enforcement:

1. The Biden administration issued Executive Order 13990, Protecting Public Health and the Environment and Restoring Science to Tackle the Climate Crisis, instructing federal agencies to review regulations issued during the Trump Administration to ensure that agency activities related to public health and the environment are based on “the best science.”35

2. The DOL cited stakeholder response which questioned whether the rulemaking reflected the scope of an ERISA plan fiduciary’s duties of prudence and loyalty, represented a

34 Eversheds Sutherland. Closing the Book on Continuing the ERISA “Best Interest” Debate—Is There Anything Left to Argue About? Legal alerts. February 16, 2021.

rushed process, and ignored “substantial evidence.” The DOL noted anecdotal evidence of the negative impact of the rules on “appropriate integration of ESG factors.”

The announcement signals that the Biden Administration will likely take a more permissive approach towards ESG investment usage by ERISA plans and propose new regulations to revise the existing rules in a manner more supportive of such investments. However, plan sponsors should still remain cautious, as the rules remain in place, and thus there is still a chance that a private suit could be brought by a participant. The move is reflective of everchanging attitudes towards ESG depending on the administration currently in office, which have made it difficult for plan sponsors to make long-term investment decisions in this area. As with any other fiduciary action, plan sponsors should continue to follow a prudent and well documented process when making an investment decision, as we await further regulatory clarity regarding ESG investments in DC plans.

---


Litigation Update

Not only did 2020 witness unprecedented change in our daily lives and slowing of the global economy due to COVID-19, it also set a record for the number of ERISA decisions issued by the US Supreme Court and the volume of new litigation filed under ERISA. The US Supreme Court issued four ERISA decisions, more than it has issued in any other year of the statute’s 45-year existence. Additionally, a little over 200 new ERISA class action lawsuits were filed in 2020, an increase of about 80% from 2019. Similar to prior years, a significant portion of these lawsuits alleged violations due to excessive fees.38

In recent months, DC-plan litigation continues to be driven by familiar themes: breach of fiduciary duty due to excessive fees, multiple vendors, not using lowest-fee share class, active vs. passive offerings, underperforming funds—not only for large sponsors but increasingly for smaller retirement plans (less than $100 million in assets and under 1,000 participants) as well. Other allegations observed include offering a particular mix of investment options, choice of investment vehicle (mutual fund vs. collective investment trusts and separate accounts), selection and monitoring of target date funds, proprietary funds, single stock funds, required contents of COBRA notices, cybersecurity, arbitration clauses and class action waivers, actuarial assumptions, employee stock ownership plans, and health plans, among others.

Plan sponsors should maintain awareness of DC retirement plan litigation trends. Although there is no particular course of action that a plan sponsor can take to avoid the threat of litigation, following general fiduciary and governance best practices, such as using a prudent decision-making process, periodic review of investment offerings, compliance and adherence to plan documents, periodic review and monitoring of service providers, and maintaining proper and complete documentation of fiduciary decisions, can be helpful to limit risk.

Below are summaries of recent high-profile cases that plan sponsors should be aware of:

**Sulyma vs. Intel/ Anderson v. Intel Corp. Investment Policy Committee**

January 2021 saw a ruling in the closely watched case of Anderson v. Intel Corp. Investment Policy Committee, which looked at the ability of plan sponsors to include alternative investments in 401(k) target date funds. The case was consolidated with a lawsuit filed by Christopher Sulyma that had made it to the Supreme Court in 2020 on a technical issue regarding the statute of limitations to file a claim under ERISA (decided in the plaintiff’s favor). Following the Supreme Court’s ruling, the case was sent back to the lower courts for further arguments on the merits of the claim.39

The long running case, originally filed in 2015, accused Intel of ERISA violations for its plan management and the use of hedge funds and private equity. The case alleged that the Intel investment committee breached its duty under ERISA by adopting an asset allocation model with

---

a high allocation to non-traditional investments (hedge funds and private equity) in the retirement plan’s target date funds and Intel Global Diversified Fund, which exposed the participants to considerable risk for comparatively higher fees and poor performance compared to their peers. The suit included allegations of self-dealing for the use of private equity funds in which Intel Capital also invested. It also claimed that plan participants were not provided material and accurate risk and fee disclosures and that the funds would not have suffered losses if asset allocation models were consistent with prevailing standards for investment experts and prudent fiduciaries.40

A US District Court for the Northern District of California dismissed the claims due to the plaintiff’s failure to provide sufficient evidence that the alternative investments were imprudent. The plaintiffs were not able to provide adequate support for establishing the benchmarks for ‘peer’ and ‘comparable’ funds to compare the performance and fees of the Intel funds. The judge pointed out, “ERISA requires that fiduciaries act prudently, but it does not require that fiduciaries mimic the industry standard when making investments” in response to the plaintiff’s argument that Intel fiduciaries “drastically departed from prevailing standards of professional asset managers.”41 The plaintiff also did not provide factual allegations to support a claim that the committee invested in certain private equity funds to aid Intel Capital in its venture capital investments.

The decision has been seen as raising the bar for plaintiffs looking to challenge the offering of non-traditional investment strategies. The court’s decision also reaffirms that plan fiduciaries should continue to employ and adhere to a diligent investment evaluation and selection process that includes documenting the rationale for asset class/ fund selection and a given investment’s appropriateness for plan participants.

Hughes et al. vs. Northwestern University et al.

It was announced recently that the US Supreme Court will hear oral arguments this fall for an ERISA case against Northwestern University brought by participants in two of the university’s 403(b) plans alleging excessive investment and record keeping fees. The case, for which a decision is expected in 2022, could have ramifications, both for existing lawsuits against colleges and universities and for plan fiduciaries in general, regarding standards for the selection and monitoring of investment options and service providers.42

The initial complaint was filed in August 2016 against the fiduciaries for breach of fiduciary duty of prudence under ERISA for having multiple recordkeepers, resulting in high fees and offering too many investment options, as well as offering retail share classes instead of institutional share classes. The U.S District Court for the Northern District of Illinois dismissed the suit in May 2018 for failure to plausibly allege a breach of fiduciary duty of prudence, which was affirmed by the US Court of Appeals for the Seventh Circuit in March 2020.43

40 Ropes & Gray. 3 Takeaways from Intel Retirement Plan Leaders’ ERISA Win. Alerts. February 18, 2021.
41 Steyer, Judge Says Intel ERISA Suit Does Not Compute.
43 Baldwin, Samuel. JD Supra. Supreme Court Will Hear Northwestern University 403(b) Plan Excessive Fee Case. July 13, 2021.
The case is one of many that have been filed against large universities in recent years. Another case, against University of Pennsylvania, was originally dismissed by the District court but was subsequently reversed-in-part by the US Court of Appeals for the Third Circuit.

As a result of the inconsistency, the Northwestern University plaintiffs argued that the Seventh Circuit’s decision created a circuit split that warranted review by the Supreme Court. In addition, the Acting Solicitor General filed a brief at the Court’s request concluding that the Seventh Circuit opinion was wrongly decided and asking the Supreme Court to take the case due to the discrepancy and because “[a]t least two of the [Northwestern plaintiffs’] claims…state a plausible claim for breach of ERISA’s duty of prudence.” The two claims cited were not offering the lowest fee share class available and failing to monitor and reduce recordkeeping fees. The Supreme Court may also address other issues including investment benchmarks, investment lineup, passive funds and revenue sharing.

This case will be followed closely, as the decision could bring some clarity to the pleading standard for breach of fiduciary duty allegations related to plan expenses and investment options.

**Barnett vs. Abbott Laboratories et al**

With increased cases of cybercrime, plan sponsors, plan fiduciaries, and recordkeepers need to be extra vigilant against emerging cyber threats in order to safeguard the personal and financial data of retirement plan participants. An ongoing lawsuit filed alleging fiduciary and legal responsibility related to the loss of retirement account funds due to fraud is of significant prominence, as it may provide insight into fiduciary duties related to cybersecurity.

In Barnett vs. Abbott Laboratories et al, a former employee of Abbott Laboratories (“Abbott Labs”) sued Abbott Labs and the plan’s recordkeeper, Alight Solutions (“Alight”) after an imposter stole $245,000 from her account. The lawsuit, filed in April 2020, alleged that both Abbott Labs and Alight breached their fiduciary duties of loyalty, prudence and monitoring by failing to take the necessary steps to protect the plan’s assets. In addition, the complaint alleged Alight’s violation of the Illinois Consumer Fraud and Deceptive Business Practice (ICFA).

In October 2020, the US District Court for the Northern District of Illinois dismissed the claim against Abbott Labs, while it rejected the dismissal request by Alight. The judge found that the complaint against Abbott Labs failed to demonstrate that Abbott Labs was a fiduciary to the plan. The plaintiff also failed to provide evidence of the Abbott Lab plan administrator (who the court agreed was a fiduciary) breaching their fiduciary duty. The judge denied Alight’s motion to dismiss as “there are sufficient allegations on the face of the complaint to infer that Alight acted as a

---


fiduciary by exercising discretionary control or authority over the plan’s assets.” The court granted permission for the ERISA and the state law claims to proceed against Alight. Alight has since responded to the compliant, agreeing with much of the description of the theft but denying fiduciary status or any liability for the plaintiff’s losses.

Following the Court’s decision, the plaintiff filed an amended complaint against Abbot Labs for its initial hire of Alight in 2003 and subsequent renewal of its contract in 2015, which were again dismissed. The Court noted that Alight was first hired before the plaintiff’s theft took place and the two identified incidents that happened prior to the renewal were limited in size and scope, and neither of the events involved Alight’s performance on behalf of the Abbott Lab’s plan. However, the Court has asked the plan sponsor to complete its document production as part of the discovery process, and the plaintiff can choose to file a second amended allegation if the prior deficiencies in her filing can be addressed.

Although claims against the plan sponsor have been dismissed for now, the lawsuit demonstrates the imperative that fiduciaries understand and monitor the cyber security policies and procedures of their service providers, especially processes for plan withdrawals and distributions, as well as educate participants on steps they can take to limit cybersecurity risks. As discussed earlier, the DOL recently provided helpful cybersecurity guidance to plan sponsors, plan service providers, and plan participants.

---

48 Adams, *Split Decisions in 401(k) Theft Suit for Plan Sponsor*, RK.
References


https://www.groom.com/resources/dol-issues-missing-participants-guidance/


https://www.plansponsor.com/house-education-labor-committee-debates-secure-2-0/


Ropes & Gray. 3 Takeaways from Intel Retirement Plan Leaders’ ERISA Win. Alerts. February 18, 2021. 


https://www.dol.gov/newsroom/releases/ebsa/ebsa20210414

https://www.dol.gov/newsroom/releases/ebsa/ebsa20210212

https://www.dol.gov/newsroom/releases/ebsa/ebsa20210112

https://www.dol.gov/newsroom/releases/ebsa/ebsa20210310

**Disclaimer**

*The views expressed in this commentary reflect those of RVK, Inc. (RVK) as of the date of this commentary. These views are subject to change at any time based on market, industry, regulations, or other conditions, and RVK disclaims any responsibility to update such views. Nothing in this commentary is intended as legal or tax advice. In preparing this commentary, we have used sources that we believe reliable but cannot guaranty their accuracy.*