KANSAS BOARD OF REGENTS
Retirement Plan Committee
October 19, 2021

AGENDA

Kansas Board of Regents
Retirement Plan Committee
October 19, 2021, at 1:30 p.m.

1. Approve: Minutes from March 16, 2021, and June 15, 2021

2. Introduction of new members: Regent Harrison-Lee, Chair, and Jeff DeWitt, COBO representative

   A. Introductions from TIAA, Voya and ACG
      i. TIAA: Katie Skorupski, Senior Relationship Manager; Byron Blaine, Senior Director Advisory and Financial Consulting; Brock Noel, Managing Director
      ii. Voya: Cindy Delfelder, Client Relations Manager, and John O'Brien, Regional Vice President
      iii. ACG: Brad Tollander and Justin Dorsey
   B. Introductions of RPC members

3. Review of Fiscal Year 2021 Mandatory and Voluntary Plan expenses – Natalie Yoza

   A. **Vote** on recommendations to Board for formula for billing Mandatory and Voluntary Plan expenses and approval of Fiscal Year 2021 Plan expenses
   B. **Vote** on proposal to recommend the Board amend the RPC Charter

4. Legal Services Update – Natalie Yoza

   A. **Vote** on proposed spending limit for legal services
   B. **General consensus** approval to begin the RFP process related to third-party administrative services

5. TIAA settlements with NY Attorney General and the Securities and Exchange Commission – TIAA, Brock Noel, Managing Director

6. Cybersecurity – Justin Dorsey, ACG

   A. **Vote** on proposal to approve updating recordkeeper contracts to include cybersecurity addendums

7. ACG semi-annual reports through 6/30/21 – Brad Tollander

8. Good of the Order

9. Next meeting March xx, 2022

KANSAS BOARD OF REGENTS
Retirement Plan Committee (RPC)
MINUTES
March 16, 2021

The March 16, 2021, video conference meeting of the Kansas Board of Regents Retirement Plan Committee was called to order at 12:30 p.m.

Members Participating:

Regent Shane Bangerter, Chair	Debbie Amershek, PSU
Mike Barnett, FHSU	Dipak Ghosh, ESU
Dr. Rick Lecompte, WSU	Stacey Snakenberg, KUMC
Jay Stephens, KSU	Madi Vannaman, KBOR

President Steve Scott was unable to participate. Participating from Advanced Capital Group were consultants Brad Tollander and Justin Dorsey. Also participating, from TIAA: Nicolette Dixon, Senior Relationship Manager; Katie Skorupski, Senior Relationship Manager; and Kendra Kamesch, Senior Manager Communications Consultant; and from Voya, John O'Brien, Regional Vice President; and Cindy Delfelder, Relationship Manager; and from the Board Office: Natalie Yoza, Associate General Counsel, and Elaine Frisbie, Vice President Administration and Finance.

Minutes
Dipak Ghosh moved to approve the minutes from the September 8, 2020. Following the second of Rick LeCompte, the motion carried.

Retirement plan contributions correction issue
Natalie Yoza shared information about an issue impacting one university and the incorrect application of the 15-year catch-up provision allowed by the IRS over a five-year period (from 2014 to 2019). The university conducted an audit through each year until they found consecutive years without excess contributions. By identifying the error's source, training materials were created to ensure this would not occur again. The university partnered with a public accounting firm to complete tax amendments for any of the 108 impacted employees who needed assistance and reimbursed any late fees and IRS assessed penalties. The university also worked with legal counsel to ensure IRS compliance. This error was eligible for self-correction under the IRS' correction program and the Board of Regents is not required to file a correction with the IRS or to pay a fee.

ACG semi-annual report through 12/31/20
Brad Tollander presented highlights from the semi-annual report. The Executive Summary included review of items discussed at the September 2020 RPC meeting. ACG reviewed the one-year progress of the two funds placed on the Watch List at the Spring 2019 RPC meeting: TIAA-CREF Large-Cap Value Institutional and TIAA-CREF Mid-Cap Value Institutional.

TIAA-CREF Large-Cap Value Institutional (Large Cap Value Option)
ACG recommended keeping this fund on Watch. Near-term performance results have improved under the new manager. ACG's preference is to see meaningful improvement in the fund's long-term relative performance results and management team stability before recommending removal from Watch. This fund will be evaluated again at the Fall 2021 RPC Meeting.

TIAA-CREF Mid-Cap Value Institutional (Mid-Cap Value Option)
This fund has gone through two management team and strategy changes in the past three years. The current team has managed since January 17, 2020, and the fund underperformed severely relative to peers and benchmark during their tenure. While all active managers can be expected to go through periods of underperformance, this fund's team and strategy instability, as well as continued underperformance after team changes, warrants a fund search.

TIAA provided ACG with a number of mid-cap value options to evaluate. ACG narrowed the list to a manageable number by reviewing risk-adjusted performance, consistency of performance, management team and fees. ACG's recommendation is to replace this fund with the John Hancock Disciplined Value Mid Cap R6 fund due to the management and strategy instability and continued poor performance.

ACG's rationale for this change:

- Long-tenured strategy which balances a quantitative and fundamental process. The team narrows down options using three components: relative value (40%), momentum (40%), and business health (20%) reinforced with fundamental research. As a result, this fund tends to hold a quality bias relative to peers.
- Strong trailing, rolling and risk-adjusted performance numbers. Strongest consistency of performance when measured against the other managers.
- Strong Sharpe Ratio (defined as return per unit of risk) metrics over the long-term as well as over three-and five-year rolling periods relative to peers and benchmark.
- Tenured management team which has consistently executed the strategy for 20 years.

Rick LeCompte moved to replace the TIAA-CREF Mid-Cap Value Fund with the John Hancock Disciplined Value Mid Cap R6 Fund (JVMRX) in both the Mandatory and Voluntary Plans. Following the second of Dipak Ghosh, the motion carried.

Provider Lineup Recommendations
Voya was the only company that made a recommendation for a fund lineup change to replace the current suite of Vanguard Target Retirement Investor Share class funds with the less expensive Institutional share class.

Vanguard's Target Retirement funds added an Institutional share class in June 2015. This series is identical in underlying index options and glidepath methodology but uses lower fee versions of the index funds and, as a result, has a significantly lower expense ratio for every vintage relative to the Investor share class. Effective December 11, 2020, Vanguard lowered the minimum investment for the Institutional share class of their target date suite from $100 million to $5 million. This change allows the plan to access this share class, which would lower fund expenses from 12-15 bps to 9 bps.

ACG agrees with that recommendation and also recommends adding the 2065 vintage, which will be appropriate for employees age 20-25 and/or employees who plan to retire in the year 2065, to both the KBOR Mandatory and Voluntary Plans.

Rick LeCompte moved that the Vanguard Target Retirement Investor share class funds be moved to the Institutional share class funds and to add the 2065 fund in both the KBOR Mandatory and Voluntary Plans. Following the second of Dipak Ghosh, the motion carried.

It was noted that the TIAA-CREF Lifecycle 2065 Institutional Fund (TSFTX) will automatically be added to the Plans in the second quarter to complete the suite. Funds in the lifecycle suites can be automatically added to the Plans.

RFP for Legal Services

Natalie Yoza presented the recommendation to ask the State's Procurement Office to issue a Request for Proposals (RFP) for retirement plan legal services. Several issues have arisen that demonstrate having a contract with legal counsel would be advantageous because State procurement laws make it challenging to hire counsel quickly each time an issue arises. The Retirement Plan Committee (RPC) would need to approve issuing the RFP and the statement of work. The RPC would then form a subcommittee. the Procurement Negotiating Committee (PNC), and one RPC member would serve as a named representative with the State's Procurement Office. Once bids are received, the PNC would make a recommendation to the RPC for approval. A proposed statement of work was reviewed.

If the RFP is posted soon, questions are received from vendors, and responses submitted, bids would close around the end of April at the latest. The PNC would have up to 30 days to review the technical responses and submits its review, the Procurement Office will provide the cost proposals. The PNC would make a recommendation to the RPC and the contract can be negotiated. Once the final selection is made, the Procurement Office finalizes the contract for signature. The goal would be to have a virtual RPC meeting at the end of May to review the PNC's recommendation.

Mike Barnett moved, and Stacey Snakenberg seconded the motion that the Board staff contact the State's Procurement Office to issue a Request for Proposals for retirement plan legal services based on the statement of work included in the issue paper and recommended that Natalie Yoza and Mike Barnett be named members of the Procurement Negotiating Committee. The motion also included the RPC establishing a subcommittee to review the responses and make a recommendation to the RPC.The members of the subcommittee will be Dipak Ghosh, Rick LeCompte, Stacey Snakenberg and Madi Vannaman.

Reports on various items

A. Voya's Voluntary Plan self-directed brokerage account

With the first pay period in January 2021, the KBOR Voluntary Plan was consolidated to two vendors: TIAA and Voya. The new contracts included a number of benefits for participants, including reduced Plan pricing. For the TIAA contract, the new terms included a reduction in the Mandatory and Voluntary Plan pricing from .06% to .055%. And Voya reduced its pricing on the Voluntary Plan from .50% wrap plus a .75% revenue share to .12%.

The intent was to maintain the self-directed brokerage account with TIAA and to add a self-directed brokerage account for Voya participants. However, negotiations stalled with Voya's subcontractor, TD Ameritrade, because Ameritrade would not accept the Kansas Department of Administration's DA-146a (Rev. 07-19) addendum, which contains the standard terms required by the State including language that agencies will not agree to indemnify any contractor or third party for any acts or omissions. If these circumstances change, a self-directed brokerage account will again be pursued for Voya participants.

The self-directed brokerage account continues to be available for TIAA participants. As of March 2, 2021, there were 17 accounts with a total balance of $829,259. Three accounts belong to participants

who are no longer employed, and six of those accounts contain less than $100.00. This means there is low utilization, but the option continues to be available.

B. Planwithease complaint
Since 2008, Planwithease (PWE) has been the KBOR third-party administrator to authorize distributions for qualifying participants. A participant wanted a roll-over distribution and needed to obtain the PWE certificate which establishes eligibility to access funds. The certificate remains active for 30 days and is to be submitted along with the retirement company's distribution forms. Because the participant began trying to get distribution in April 2020, and was successful in August 2020, the participant is claiming losses because of the delay. The participant received the certificate from the employing university but did not process it within the 30-day period. While the participant struggled with securing the certificate on-line, the university HR offices now have the ability to get and email the certificates to participants and PWE also is now able to overnight the certificates to participants.

The KBOR Office is trying to ensure that participants have an easy and efficient process to get the certification for distribution but also to ensure that privacy and confidentiality is maintained to meet legal obligations. Looking toward the future, Natalie Yoza recommended a possible RFP to ensure due diligence to review available options to meet distribution requirements.

C. COVID-related distributions (CRDs)
Information about KBOR 403(b) Plan distributions that occurred the Coronavirus Aid, Relief, and Economic Security Act (CARES Act) was shared. There were 657 CRDS taken and about 30% of those were for participants with more than one request. The total amount distributed was $13,995,471 and 97% of those distributions were from the Mandatory Plan.

TIAA and Voya – Retirement Guide
At the September 2020 RPC meeting, custom concepts were discussed, and the RPC requested that TIAA and Voya develop a Retirement Guide using those concepts. Once finalized, the Retirement Guide will replace the current Your Future, Your Choice brochure. It will be posted on the KBOR website and will be provided to the campuses to share with faculty and staff newly eligible for the KBOR retirement plans.

Good of the Order
1. Nicolette Dixon, who is moving into a different role within TIAA, expressed her appreciation for the RPC and the KBOR universities for making her feel a part of our family and for pouring into her many values and ideas that have enabled her to take her career to the next level. Nicolette is TIAA's Director of Communications and National Advocacy, and will be working with CUPA-HR, NACUBO and presidential and women's associations Nicolette quoted Maya Angelou: "People will forget what you said, people will forget what you did, but people will never forget how you made them feel." Nicolette's strong advocacy for KBOR, her professionalism and engaging personality will be missed!

Next RPC meeting:
The next regular RPC meeting will be scheduled for September 2021 TBD.

KANSAS BOARD OF REGENTS
Retirement Plan Committee (RPC)
MINUTES
June 15, 2021

The June 15, 2021, video conference meeting of the Kansas Board of Regents Retirement Plan Committee was called to order at 12:03 p.m.

Members Participating:
Regent Shane Bangerter, Chair
Dipak Ghosh, ESU
Stacey Snakenberg, KUMC
Madi Vannaman, KBOR
Debbie Amershek, PSU
Dr. Rick Lecompte, WSU
Jay Stephens, KSU

Mike Barnett was unable to attend the meeting, Julene Miller, Board Counsel was also present.

At 12:05 p.m., Rick LeCompte moved, followed by the second of Dipak Ghosh, to recess into executive session for 45 minutes to discuss matters deemed privileged in the attorney-client relationship. The subject of this executive session was to evaluate proposals for legal services negotiated pursuant to K.S.A. 75-37,102 and the purpose is to maintain the confidentiality of the proposals during the negotiation process. Participating in the executive session were members of the Retirement Plan Committee, Madi Vannaman, Board Staff Affiliate for Benefits and Retirement Plan Administrator and Julene Miller, Board Counsel. The motion carried. At 12:35 p.m., the meeting returned to open session.

Good of the Order:
The Retirement Plan Committee recognized and thanked Regent Bangerter for his leadership as chair of the Committee from 2017 to 2021.

The meeting was adjourned at 12:55.

Act on (1) Formula for Deducting Authorized Expenses from Revenue Accounts and Distributing Excess to Retirement Plan Participants and (2) Fiscal Year 2021 Expenses

Summary and Staff Recommendation

Due to the Retirement Plan Committee's new oversight of the Voluntary Retirement Plan, the formula for deducting authorized Plan-related expenses from the revenue sharing accounts with TIAA and Voya needs to be reconsidered along with how the remaining funds are distributed back to Plan participants. Board staff propose that the RPC recommend the Board allocate expenses between TIAA and Voya pro rata based on the number of active Mandatory and Voluntary Plan participants and distributing the remaining revenue account balance pro rata based on the participant's account balances in the Mandatory and Voluntary Plans.

The Fiscal Year 2021 expenses must be reviewed for reasonableness and a recommendation made to the Board regarding approval. These expenses must be billed to the revenue sharing account by December 31, 2021. The invoice is attached.

The Formula for Deducting Expenses and Distributing the Excess to Plan Participants

The Board's contracts with TIAA and Voya establish revenue sharing accounts so that authorized Plan-related expenses (such as consulting fees, Board Office salary and overhead expenses, and legal fees) can be billed to the retirement plans. The recordkeepers place excess revenue in the revenue sharing account, the Board's authorized Plan-related expenses are deducted annually from each company's revenue account, and the remaining funds are distributed back to participants. Notably, Voya also has a $50,000 special fund for plan expenses that is used first. Because it is not funded from Plan assets, the unused funds go back to Voya.

Historically, revenue sharing has occurred on the Mandatory Plan. Now that the RPC has additional oversight of the Voluntary Plan, the formulas must be reviewed. This process must be completed by December 31, 2021.

The first step is to allocate expenses to the Mandatory or Voluntary Plan. The contract for Advanced Capital Group (ACG) establishes the additional expenses associated with the Voluntary Plan's oversight. And Ice Miller—the new law firm for the Plans—will note which Plan should be billed on any invoices. However, Board office expenses will need to be allocated between the Plans. Board staff recommend allocating these expenses proportionally based on the number of participants in the Plans.

The second step is to allocate expenses for both the Mandatory and the Voluntary Plans between the two recordkeepers. In 2013, the Retirement Plan Committee (RPC) voted to allocate expenses between the recordkeepers proportionally based on the number of active Mandatory Plan participants. The number of active participants is determined annually using a May pay period to include academic year faculty participation because many are on leave during the summer. Board staff recommend the same approach for the Voluntary Plan, *i.e.*, allocating expenses to TIAA and Voya based on the number of active participants in the Voluntary Plan.

Participation #s as of 5/28/21	TIAA	% of Total	Voya	% of Total	Total # of Participants	KBOR invoice total
Mandatory	9,578	73%	3,474	27%	13,052	$ 85,354.66
Voluntary	2,147	68%	995	32%	3,142	$ 31,848.26

In 2012, the RPC determined that the remaining funds in the revenue accounts should be distributed to Plan participants pro rata based on their account balance. Board staff recommend using the same formula based on a participant's account balance in the Voluntary Plan. Because participants with a higher account balance paid a higher proportion of the fees, this ensures a more equitable distribution of the excess revenue.

Fiscal Year 2021 Expenses

Federal law permits using retirement plan assets to pay for certain approved expenses required for administration of the retirement plans. The expenditure must be prudent, and the amount must be reasonable. The attached invoice itemizes the Fiscal Year 2021 Plan expenses. The following chart applies the above formula to deduct those expenses from the revenue sharing accounts and identifies the excess revenue that will be distributed back to Plan participants. To deduct these expenses before December 31, 2021, the RPC needs to make a recommendation to the Board for approval at the November Board meeting.

TIAA (1)	Revenue Account Balance	KBOR Plan Expenses	Balance for Plan Account Holders
Mandatory Plan	$ 857,151.54	$ 62,636.14	$ 794,515.40
Voluntary Plan	$ 276,343.86	$ 21,762.64	$ 254,581.22
	$ 1,133,495.40	$ 84,398.78	$ 1,049,096.62

Voya (2)	Revenue Account Balance	KBOR Plan Expenses Exceeding $50,000 (see Note 3)	Balance for Plan Account Holders
Mandatory Plan	$ 107,130.46	$ -	$ 107,130.46
Voluntary Plan	$ 488.45	$ -	$ 488.45
	$ 107,618.91		$ 107,618.91

(1) TIAA Revenue Account information as of 10/7/21

(2) Voya Revenue Account information as of 10/8/21

(3) Voya has allocated a $50,000 Special Plan Payment to pay for Plan expenses before the Revenue Account is used. Since the FY 2021 Plan Expenses total less than $50,000, the Special Plan Payment will pay those expenses.

Voya Special Plan Payment	
Special Plan Payment Balance	$ 50,000.00
Mandatory Plan Expenses	$ (22,718.52)
Voluntary Plan Expenses	$ (10,085.62)
Balance	$ 17,195.86

Kansas Board of Regents
Retirement Plan Actual Annual Expenditures
FY 2021

10/6/2021

Expense Categories	Agency Expense	Percentage Applied	Mandatory Plan	Voluntary Plan	Invoice Amount
Salaries [1]					
Madi	22,286.93	22,286.93	17,962.76	4,324.17	22,286.93
Julene	132,465.78	1,324.66	1,067.65	257.01	1,324.66
Natalie	112,245.50	11,224.55	9,046.74	2,177.81	11,224.55
Renee	71,670.57	716.71	577.65	139.06	716.71
Elaine	208,632.79	2,086.33	1,681.54	404.79	2,086.33
Bangerter	192.40	192.40	155.07	37.33	192.40
September 8, 2020, March 16, 2021					
Salaries Total		$ 37,831.58	$ 30,491.41	$ 7,340.17	$ 37,831.58
Investment and Legal Consultants					
Advanced Capital	61,000.00		41,000.00	20,000.00	61,000.00
Ice Miller	3,000.00		1,500.00	1,500.00	3,000.00
Investment and Legal Consultants Total	$ 64,000.00		$ 42,500.00	$ 21,500.00	$ 64,000.00
Travel [2]					
Madi Vannaman					
Shane Bangerter					
Elaine Frisbie					
Travel Total [3]	$ -		$ -	$ -	$ -
Other direct expenses (mailings, conference calls)					
Secretary of State Legal Pub tax sheltered annuity pr	84.00		42.00	42.00	84.00
Other direct expenses Total	$ 84.00		$ 42.00	$ 42.00	$ 84.00
Direct Expenses Total	$ 101,915.58		$ 73,033.41	$ 28,882.17	$ 101,915.58
Indirect (F&A, IT, office space) 15%		$ 15,287.34	12,321.25	2,966.09	15,287.34
Total Expenses			**$ 85,354.66**	**$ 31,848.26**	**$ 117,202.92**
Cost per participant			$ 6.54	$ 10.14	

Notes:

1. Salaries - included the portion that KBOR paid for KU staff affiliate salary from retirment plan admin account; 10% of KBOR Associate General Counsel; 1% General Counsel; 1% Legal Assistant; 1% VP of Finance & Administration; Regent members salary for 2021 meetings attended.

2. Travel - included 2/3 of KU staff affiliate travel expenses; Regents members travel; VP Fin & Admin travel

3. No travel FY2021 due to COVID restrictions

Act to Recommend that the Board Amend the Retirement Plan Committee Charter to Delegate Responsibility for Reviewing Reasonableness of Plan Expenses

Summary and Staff Recommendation

The "Retirement Plan Committee" (RPC) is a Board created co-fiduciary for the Mandatory and Voluntary Retirement Plans. The Board established the RPC to assist with oversight of Plan investments and administration of the Plans. The Board Policy Manual establishes the RPC, and the RPC's Charter further defines the Committee's mission and functions. Board staff propose that the RPC seek an amendment to the Committee's Charter delegating to the RPC the fiduciary responsibility to review that all services provided to the plans are necessary and that the cost of those services is reasonable.

Background on the Kansas Board of Regents Retirement Plans

The Board's Policy Manual creates the Retirement Plan Committee (RPC), stating it is "responsible for issues related to the Board's retirement plan, including oversight of plan investments and administration."[1] The RPC reports directly to the Board, and it has authority to initiate issues related to the Mandatory and Voluntary Plans.

The RPC's Charter further defines the Committee's authority and responsibilities for the Plans. It establishes that the RPC members are fiduciaries to the Plans and assigns certain oversight tasks. Those tasks include: (1) ensuring proper due diligence in selection of investment managers and/or investment funds; (2) developing and periodically reviewing investment policies and procedures; and (3) retaining outside experts, as needed, to assist in the development and monitoring of the overall investment program.[2] Board approval is required to amend the RPC Charter.[3]

Recommended Changes to the RPC Charter

Board staff propose that the RPC recommend to the Board that it amend the Committee's Charter to delegate the fiduciary duty to review that all services provided to the Plans are necessary and that the cost of those services is reasonable.

This additional responsibility would be added to the section of the Charter titled "Mission Statement and Principal Functions," and it would state:

> "Specifically, the Committee shall be responsible for the following:
>
> - Ensure that proper due diligence is conducted in the selection of investment managers and/or investment funds.
> - Monitor and evaluate performance results achieved by the investment managers.
> - Establish effective communication procedures between investment managers, investment funds, external parties (such as consultants), Plan participants and campus administrators and the Committee.

[1] Board Policy Manual, Chapter I, Section A.4.a.iii.
[2] RPC Charter, page 3.
[3] RPC Charter, page 4.

- Develop and periodically review investment policies and procedures.
- Provide ongoing communications with the Board.
- Conduct periodic Committee meetings.
- Retain independent outside experts, as needed, to assist in the development and monitoring of the overall investment program.
- Administer and carry out the provisions of the plans.
- Delegate appropriate individuals and engage third parties to carry out plan provisions where appropriate.
- Approve and adopt plan documents and material amendments and modifications (subject to any further approval requirements of the Board).
- Approve amendments and interpretations of plan provisions other than those indicated above.
- Address questions concerning the eligibility, provisions, and features of the plans, including elections, contributions and benefits.
- Ensure required notices and information are distributed to participants.
- Establish procedures for enrollment, payroll deductions, distributions, and rollovers under the plan.
- Review that all services provided to the plans are necessary and that the cost of those services is reasonable.
- Such other duties and responsibilities as may be assigned to the Committee, from time to time, by the Board, or as designated in plan documents and/or investment policy statement."

Q2 2021 FACTS & STATS

Helping secure the future for millions

TIAA was founded in 1918 to help teachers retire with dignity. That mission grew to include those in healthcare and more, creating reliable income for their futures while they work to make a difference today.

Our commitment to doing the right thing—for our customers, employees and communities—has never wavered, and is why today, we're an industry leader in building financially sound futures.

Recognized financial strength

#1 not-for-profit retirement market provider in assets and participant accounts[5]

Among the **highest rated insurance companies** in the U.S. by four leading rating agencies[6]

600+ registered representatives[7]

204 offices in **23** countries

Approx. **15,000** associates[1]

15,000+ client institutions[2]

5 million unique customers

$1.3T in assets under management[3]

$3.6B paid to retirees in 2020

$505B+ in benefits paid since 1918[4]

Proven performance

Refinitiv Lipper has named TIAA a **Best Mixed Assets Large Fund Company** for five consecutive years[8]

TIAA Traditional Annuity has credited additional amounts every year since 1948[11]

TIAA is the **largest manager** of qualified plan stable value assets at **$183.5** billion[12]

Ranked #1 for participant and life & annuity consumer websites[13]

Morningstar ratings

91% of **TIAA-CREF mutual funds** and **CREF annuities** have expense ratios below the median in their respective categories[9]

70% have received an overall rating of **4 or 5 stars** across all asset classes[10]

Real estate

#1 manager of farmland assets and a **Top 5** largest commercial real estate manager worldwide.[14,15]

Unmatched dedication

To our employees

Named a **World's Most Ethical Company** seven consecutive years[16]

Awarded a **100%** rating on the **Corporate Equality Index**[17]

Listed on

100 Best Companies for Working Mothers[18]

Top 70 Companies for Executive Women[19]

Top 50 Companies for Diversity[20]

To our communities

#1 U.S. supporter of shareholder proposals on diversity, inclusion and social justice[21]

16,700+ community volunteer hours logged by employees[22]

And our planet

Top 5 Sustainable Fund asset manager[23]

Committed to **zero carbon emissions** by 2050 for the TIAA General Account

1. Includes TIAA affiliate companies.
2. Includes unique institutional clients serviced by TIAA for either retirement or Keogh plans (prior versions of this fact-sheet utilized a more broadly inclusive definition of "institutions").
3. As of June 30, 2021 assets under management across Nuveen Investments affiliates and TIAA investment management teams are $1,331 billion.
4. As of December 31, 2020. Other benefits from TIAA include: surrender benefits and other withdrawals, death benefits, health insurance and disability insurance benefits, and all other policy proceeds paid.
5. Based on data from 53 providers in PLANSPONSOR magazine's 2020 DC Recordkeeping Survey, combined 457, 403(b) and money purchase plan data as of July 15, 2020.
6. For stability, claims-paying ability and overall financial strength, Teachers Insurance and Annuity Association of America (TIAA) and TIAA-CREF Life Insurance Company (TIAA Life) are one of only three insurance groups in the United States to currently hold the highest possible rating from three of the four leading insurance company rating agencies: A.M. Best (A++ rating affirmed as of July 2020), Fitch (AAA rating affirmed as of November 2020) and Standard & Poor's (AA+ rating affirmed as of August 2020) and the second-highest possible rating from Moody's Investors Service (Aa1 rating affirmed as of May 2021). There is no guarantee that current ratings will be maintained. Ratings represent a company's ability to meet policyholders' obligations and do not apply to any product or service not fully backed by the issuer's claims-paying ability. The ratings also do not apply to the safety or the performance of the variable accounts or mutual funds, which will fluctuate in value.
7. Includes all Wealth Management Advisors and Financial Consultants
8. The Refinitiv Lipper Fund Awards are based on the Lipper Leader for Consistent Return rating, which is a risk-adjusted performance measure calculated over 36, 60 and 120 months. Lipper Leaders fund ratings do not constitute and are not intended to constitute investment advice or an offer to sell or the solicitation of an offer to buy any security of any entity in any jurisdiction. For more information, see lipperfundawards.com. Lipper Fund Awards from Refinitiv, ©2020 Refinitiv. All rights reserved. Used under license. The award pertains only to the TIAA-CREF mutual funds in the mixed-asset category. Certain funds have fee waivers in effect. Without such waivers ratings could be lower. Past performance does not guarantee future results. For current performance, rankings and prospectuses, please visit the Research and Performance section on TIAA.org. The investment advisory services, strategies and expertise of TIAA Investments, a division of Nuveen, are provided by Teachers Advisors, LLC and TIAA-CREF Investment Management, LLC. TIAA-CREF Individual & Institutional Services,LLC, and Nuveen Securities, LLC, Members FINRA, distribute securities products.
9. Based on Morningstar Direct (as of June 30, 2021) expense comparisons by category, excluding Money Market products. Actual percentage is 90.5%. TIAA-CREF mutual fund and CREF variable annuity products are subject to various fees and expenses, including but not limited to management, administrative, and distribution fees; our variable annuity products have an additional mortality and expense risk charge. Excludes the class W shares, which are not available for purchase by retail investors.
10. Morningstar ratings are based on each mutual fund (institutional share class) or variable annuity account's (lowest cost) share class and include U.S. open-end mutual funds, CREF Variable Accounts and the Life Funds. The Morningstar Rating™—or "star rating"—is calculated for managed products (including mutual funds, variable annuity and variable life subaccounts, exchange-traded funds, closed-end funds and separate accounts) with at least a three-year history. Exchange-traded funds and open-ended mutual funds are considered a single population for comparative purposes. The rating is calculated based on a Morningstar Risk-Adjusted Return measure that accounts for variation in a managed product's monthly excess performance, placing more emphasis on downward variations and rewarding consistent performance. Morningstar ratings may be higher or lower on a monthly basis. The top 10% of funds or accounts in each product category receive five stars, the next 22.5% receive four stars and the next 35% receive three stars. The overall star ratings are Morningstar's published ratings, which are derived from weighted averages of the performance figures associated with the three-, five-, and 10-year (if applicable) Morningstar rating metrics for the period ended June 30, 2021. Morningstar is an independent service that rates mutual funds. Past performance cannot guarantee future results. For current performance and ratings, please visit TIAA.org/public/investment-performance.
11. Past performance is no guarantee of future results. Any guarantees under annuities issued by TIAA are subject to TIAA's claims-paying ability. TIAA Traditional is a guaranteed insurance contract and not an investment for federal securities law purposes. Interest in excess of the guaranteed amount is not guaranteed for periods other than the periods for which it is declared.
12. LIMRA 1Q2Q 2020 Stable Value and Funding Agreement Product Survey. Based on a survey of 18 insurance companies and 2 banks reporting $760.4 billion in stable value amounts associated with qualified stable value assets. TIAA ranked first in total values.
13. DALBAR's WebMonitor program continuously analyzes financial services websites to evaluate their effectiveness in maximizing their online presence by incorporating content and functionality in a consistent, appealing and user-friendly manner. DALBAR regularly publishes key findings of competitive intelligence and benchmarking data, spotlighting notable trends, best practices, and industry leaders, as of end of Q1 2021.
14. Pensions & Investments, October 5, 2020. Rankings based on institutional tax-exempt assets under management as of June 30, 2020 reported by each responding asset manager.
15. ANREV/INREV/NCREIF Fund Manager Survey 2021. Survey illustrated rankings of 154 fund managers globally by AUM as of December 31, 2020.
16. 2015 - 2021. The World's Most Ethical Company assessment is based upon the Ethisphere Institute's Ethics Quotient® (EQ) framework which offers a quantitative way to assess a company's performance in an objective, consistent and standardized way. The information collected provides a comprehensive sampling of definitive criteria of core competencies, rather than all aspects of corporate governance, risk, sustainability, compliance and ethics. Scores are generated in five key categories: ethics and compliance program (35%), corporate citizenship and responsibility (20%), culture of ethics (20%), governance (15%) and leadership, innovation and reputation (10%) and provided to all companies who participate in the process. The full list of the 2020 World's Most Ethical Companies can be found at: https://www.worldsmostethicalcompanies.com/honorees/
17. Based on the Human Rights Campaign Foundation's Corporate Equality Index 2021.
18. 100 Best Companies for Working Mothers by Working Mother magazine, 2007-2020. 0.
19. Top 70 Companies for Executive Women by National Association of Female Executives, 2020.
20. One of DiversityInc's Top 50 Companies for the eighth year in a row 2015-2021.
21. How Did Fund Companies Use Their Proxy Votes to Tackle Racial Inequality in 2020?, Morningstar, 2020.
22. 16,701 hours served by associates from January 1, 2021 – June 30, 2021.
23. Morningstar Sustainable Funds U.S. Landscape Report, Feb 2021.

1743781
21TBR0333.02

Built for retirement

Over
6 million
customers

As of 12/31/2020

Providing services to the Education Market
for **53 Years**

As of 12/31/2020

Top 3
record-keeper
by # of plans

Pensions & Investments
April 2020

Innovation with a purpose

myOrangeMoney®
users contribute
34% more
than non-users

Digital solutions- Data includes retirement plan sponsored business as of 09/30/2020, 5.9% vs. 7.9%

Top rated
plan participant
web experience
for last 9 years
2011 – 2020

dalbar.com/Awards/AwardHistory

Unique culture

ETHISPHERE® WORLD'S MOST ETHICAL COMPANIES® 2014-2021

FORTUNE WORLD'S MOST ADMIRED COMPANIES® 2020

VOYA | Cares®

Great Place To Work. Certified 2020 USA

Bloomberg Gender-Equality Index 2021

HUMAN RIGHTS CAMPAIGN FOUNDATION BEST PLACES TO WORK 2021 for LGBTQ Equality 100% CORPORATE EQUALITY INDEX

Pensions & Investments BEST PLACES TO WORK IN MONEY MANAGEMENT ★★ 2019 ★★ MULTI-YEAR WINNER 2015 ★ 2016 ★ 2017 ★ 2018

VOYA® FINANCIAL

PLAN | INVEST | PROTECT

CN1256959_0722

Partnership with Kansas Board of Regents

Experience

Providing services to KBOR and your participants for more than **40** years, when, where and how they want to meet.

- ✓ **3** Voya offices in Kansas dedicated to retirement Plan services with Representatives are strategically located in Overland Park, Topeka, Manhattan, Wichita and Hays
- ✓ **All** campuses have onsite availability at any location.

Expertise

- ✓ **13** Local Representatives throughout the State with an average of **17** years experience
- ✓ Voya's local management team averages **27** years of experience.
- ✓ Voya has served education clients since **1967**

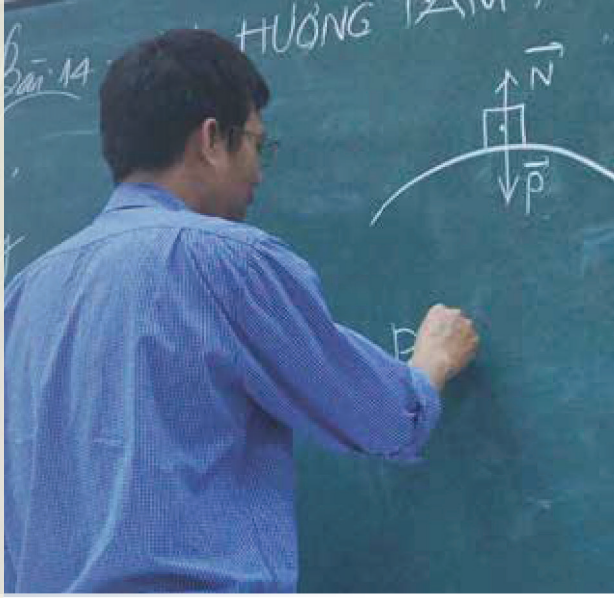
Results

- ✓ Serve **7,152** KBOR participants with over **9,000** KBOR accounts.
- ✓ Average annual contribution is **$11,512**
- ✓ Average total retirement savings for the KBOR participant is **$125,779** for the Plans compared to $94,953 for other Education plans
- ✓ **1,132** of the mandatory participants are enrolled in the Voluntary plan savings, helping drive overall retirement readiness
- ✓ Employees over the age of 70 have an average of **$291k** in combined Mandatory and Voluntary retirement savings.

VOYA® FINANCIAL

ADVANCED
CAPITAL GROUP

Retirement Plan Consulting Services



PUBLIC EMPLOYER REALITIES

Each year, employers continue to face mounting challenges:

- Complex rules and regulations followed by increasing audit activity
- Escalation of retirement plan litigation
- Complex products and service solutions
- Increased financial stress in the workforce

BENEFITS OF A PARTNERSHIP WITH ADVANCED CAPITAL GROUP

Our collaborative team provides advice based on decades of experience. We help you:

- Reduce fiduciary risk through prudent investment and governance processes
- Maximize ROI by reviewing provider services, features, and fees
- Engage employees through measurable financial wellness programs
- Implement industry best practices and strategic planning
- Alleviate your team's workload so they can focus on critical business issues

AWARD-WINNING SERVICE

Advanced Capital Group is a consulting firm and Registered Investment Advisor (RIA) based in Minneapolis, MN. Our expert team uses a proactive and collaborative approach that enhances financial results for organizations and individuals.

Dedicated to bringing plan sponsors industry best practices and helping to manage fiduciary responsibilities while creating positive outcomes for participants.

Put our vision to work for you

We are passionate about fostering creative ideas and exploring new opportunities for our clients. Contact us to learn how a customized relationship can help you succeed.

www.acgbiz.com
info@acgbiz.com
866.225.5224
50 S. Sixth Street | Suite 975
Minneapolis, MN 55402

Cybersecurity

ADVANCED CAPITAL GROUP

Department of Labor Cybersecurity Guidance (April 2021)

1. Tips for Hiring a Service Provider:
   Helps plan sponsors and fiduciaries prudently select a service provider with strong cybersecurity practices and monitor their activities, as ERISA requires.

2. Cybersecurity Program Best Practices:
   Assists plan fiduciaries and record-keepers in their responsibilities to manage cybersecurity risks.

3. Online Security Tips:
   Offers plan participants and beneficiaries who check their retirement accounts online basic rules to reduce the risk of fraud and loss.

TIAA

In December 2020 and January 2021 when file transfer software provided by Accellion was compromised and data files with personal information from several universities were made available to download on a website run by cybercriminals.

A report from email security firm Tessian looks at the state of data loss in organizations and reveals that nearly half of employees (48%) are less likely to follow safe data practices when working from home.

Voya

In an average month, we defend against 22,600,000 Threats/Month.

Recommended Next Steps

Sample Cybersecurity Tools for Small Businesses (New York State)

- Cybersecurity Policy
- Access Control Policy
- Asset Inventory & Device Management Policy
- Data Classification Policy
- Physical & Environmental Security Policy
- Risk Assessment Policy
- System & Network Security Policy
- Third Party Service Provider Policy

Service Organization Control (SOC) Audit
(https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpacybersecurityinitiative.html)

SOC 1 – Internal Controls related to financial reporting
SOC 2 – Focuses on information and IT security
SOC Cybersecurity

+ Voya's S.A.F.E.® Guarantee

Voya is committed to safeguarding your plan participants' accounts and personal information from the risk of fraud, cyber threats and unauthorized activity – so much so, we established the Voya S.A.F.E.® (Secure Accounts for Everyone) Guarantee.

What does the S.A.F.E. Guarantee mean?

If any assets are taken from your workplace retirement plan account due to unauthorized activity and through no fault of your own, we will restore the value of your account subject to you taking action to satisfy the following key steps:

1. Register your account online.
2. Review your account information on a regular basis and keep your contact information current.
3. Promptly report any suspected identity theft or unauthorized activity.
4. Practice safe computing habits.

Why the S.A.F.E. requirements?

Because we're in this fight together.

PLAN | INVEST | PROTECT

VOYA FINANCIAL

TIAA Customer Protection Policy

Safeguarding the integrity of our clients' accounts is a top priority for us. We continually monitor accounts using a combination of technology, people and processes to protect our customers, their assets and their data.

Our practice is to reinstate a client's TIAA account in full if there is a loss that is determined to be the result of unauthorized activity through no fault of the client. At the same time, it is important that clients safeguard their account information by following common security practices as outlined below. If there are indicators that a loss is attributable to client negligence, further investigation may be required before we can make a determination regarding restitution.

Your Role in Safeguarding Your Account

In an effort to keep your account as secure as possible, we ask you to take the following precautions:

- Safeguard all of your account access information.
- Avoid sharing user IDs and passwords with anyone (including family members).
- Promptly review all transaction notices and account statements for accuracy.
- Use good security practices for technology – whether you use a computer, tablet, smart phone or other digital device – to ensure you have up-to-date security protections.
- Review information on how to protect your accounts, which can be found on our Web Security Center
- Contact us as promptly as possible at **800-842-2252** or via email at abuse@tiaa.org if any unauthorized transactions are suspected, or if you suspect your personal information has been compromised.

Individual circumstances can vary. If you have reason to be concerned about access to your account, contact us and we will work with you to see whether additional account protections might be warranted.

CYBERSECURITY PROGRAM BEST PRACTICES

ERISA-covered plans often hold millions of dollars or more in assets and maintain personal data on participants, which can make them tempting targets for cyber-criminals. Responsible plan fiduciaries have an obligation to ensure proper mitigation of cybersecurity risks.

The Employee Benefits Security Administration has prepared the following best practices for use by recordkeepers and other service providers responsible for plan-related IT systems and data, and for plan fiduciaries making prudent decisions on the service providers they should hire. Plans' service providers should:

1. Have a formal, well documented cybersecurity program.
2. Conduct prudent annual risk assessments.
3. Have a reliable annual third party audit of security controls.
4. Clearly define and assign information security roles and responsibilities.
5. Have strong access control procedures.
6. Ensure that any assets or data stored in a cloud or managed by a third party service provider are subject to appropriate security reviews and independent security assessments.
7. Conduct periodic cybersecurity awareness training.
8. Implement and manage a secure system development life cycle (SDLC) program.
9. Have an effective business resiliency program addressing business continuity, disaster recovery, and incident response.
10. Encrypt sensitive data, stored and in transit.
11. Implement strong technical controls in accordance with best security practices.
12. Appropriately respond to any past cybersecurity incidents.

1. A Formal, Well Documented Cybersecurity Program.

A sound cybersecurity program identifies and assesses internal and external cybersecurity risks that may threaten the confidentiality, integrity, or availability of stored nonpublic information. Under the program, the organization fully implements well-documented information security policies, procedures, guidelines, and standards to protect the security of the IT infrastructure and data stored on the system. A prudently designed program will:

Protect the infrastructure, information systems and the information in the systems from unauthorized access, use, or other malicious acts by enabling the organization to:

- **Identify** the risks to assets, information and systems.
- **Protect each of the necessary assets, data and systems.**
- **Detect and respond to** cybersecurity events.
- **Recover** from the event.
- **Disclose the event as appropriate**.
- **Restore normal operations and services**.

Establish strong security policies, procedures, guidelines, and standards that meet the following criteria:

- Approval by senior leadership.
- Review at least annually with updates as needed.
- Terms are effectively explained to users.
- Review by an independent third party auditor who confirms compliance.
- Documentation of the particular framework(s) used to assess the security of its systems and practices.

- Formal and effective policies and procedures governing all the following:
  1. Data governance and classification.
  2. Access controls and identity management.
  3. Business continuity and disaster recovery.
  4. Configuration management.
  5. Asset management.
  6. Risk assessment.
  7. Data disposal.
  8. Incident response.
  9. Systems operations.
  10. Vulnerability and patch management.
  11. System, application and network security and monitoring.
  12. Systems and application development and performance.
  13. Physical security and environmental controls.
  14. Data privacy.
  15. Vendor and third party service provider management.
  16. Consistent use of multi-factor authentication.
  17. Cybersecurity awareness training, which is given to all personnel annually.
  18. Encryption to protect all sensitive information transmitted and at rest.

2. Prudent Annual Risk Assessments.

A Risk Assessment is an effort to identify, estimate, and prioritize information system risks. IT threats are constantly changing, so it is important to design a manageable, effective risk assessment schedule. Organizations should codify the risk assessment's scope, methodology, and frequency. A risk assessment should:

- Identify, assess, and document how identified cybersecurity risks or threats are evaluated and categorized.
- Establish criteria to evaluate the confidentiality, integrity, and availability of the information systems and nonpublic information, and document how existing controls address the identified risks.
- Describe how the cybersecurity program will mitigate or accept the risks identified.
- Facilitate the revision of controls resulting from changes in technology and emerging threats.
- Be kept current to account for changes to information systems, nonpublic information, or business operations.

3. A Reliable Annual Third Party Audit of Security Controls.

Having an independent auditor assess an organization's security controls provides a clear, unbiased report of existing risks, vulnerabilities, and weaknesses.

As part of its review of an effective audit program, EBSA would expect to see:

- Audit reports, audit files, penetration test reports and supporting documents, and any other analyses or review of the party's cybersecurity practices by a third party.
- Audits and audit reports prepared and conducted in accordance with appropriate standards.
- Documented corrections of any weaknesses identified in the independent third party analyses.

4. Clearly Defined and Assigned Information Security Roles and Responsibilities.

For a cybersecurity program to be effective, it must be managed at the senior executive level and executed by qualified personnel. As a senior executive, the Chief Information Security Officer (CISO) would generally establish and maintain the vision, strategy, and operation of the cybersecurity program which is performed by qualified personnel who should meet the following criteria:

- Sufficient experience and necessary certifications.
- Initial and periodic background checks.
- Regular updates and training to address current cybersecurity risks.
- Current knowledge of changing cybersecurity threats and countermeasures.

5. Strong Access Control Procedures.

Access control is a method of guaranteeing that users are who they say they are and that they have the appropriate access to IT systems and data. It mainly consists of two components: authentication and authorization. The following are best security practices for access control:

- Access to systems, assets and associated facilities is limited to authorized users, processes, devices, activities, and transactions.
- Access privileges (e.g., general user, third party administrators, plan administrators, and IT administrators) are limited based on the role of the individual and adhere to the need-to-access principle.
- Access privileges are reviewed at least every three months and accounts are disabled and/or deleted in accordance with policy.
- All employees use unique, complex passwords.
- Multi-factor authentication is used wherever possible, especially to access the internal networks from an external network, unless a documented exception exists based on the use of a similarly effective access control methodology.
- Policies, procedures, and controls are implemented to monitor the activity of authorized users and detect unauthorized access, use of, or tampering with, nonpublic information.
- Procedures are implemented to ensure that any sensitive information about a participant or beneficiary in the service provider's records matches the information that the plan maintains about the participant.
- Confirm the identity of the authorized recipient of the funds.

6. Assets or Data Stored in a Cloud or Managed by a Third Party Service Provider are Subject to Appropriate Security Reviews and Independent Security Assessments.

Cloud computing presents many unique security issues and challenges. In the cloud, data is stored with a third-party provider and accessed over the internet. This means visibility and control over that data is limited. Organizations must understand the security posture of the cloud service provider in order to make sound decisions on using the service.

Best practices include:

- Requiring a risk assessment of third party service providers.
- Defining minimum cybersecurity practices for third party service providers.
- Periodically assessing third party service providers based on potential risks.

- Ensuring that guidelines and contractual protections at minimum address the following:
  - » The third party service provider's access control policies and procedures including the use of multi-factor authentication.
  - » The third party service provider's encryption policies and procedures.
  - » The third party service provider's notification protocol for a cybersecurity event which directly impacts a customer's information system(s) or nonpublic information.

7. Cybersecurity Awareness Training Conducted at Least Annually for All Personnel and Updated to Reflect Risks Identified by the Most Recent Risk Assessment.

Employees are often an organization's weakest link for cybersecurity. A comprehensive cybersecurity security awareness program sets clear cybersecurity expectations for all employees and educates everyone to recognize attack vectors, help prevent cyber-related incidents, and respond to a potential threat. Since identity theft is a leading cause of fraudulent distributions, it should be considered a key topic of training, which should focus on current trends to exploit unauthorized access to systems. Be on the lookout for individuals falsely posing as authorized plan officials, fiduciaries, participants or beneficiaries.

8. Secure System Development Life Cycle Program (SDLC).

A secure SDLC process ensures that security assurance activities such as penetration testing, code review, and architecture analysis are an integral part of the system development effort. Best practices include:

- Procedures, guidelines, and standards which ensure any in-house applications are developed securely. This would include such protections as:
  - » Configuring system alerts to trigger when an individual's account information has been changed.
  - » Requiring additional validation if personal information has been changed prior to request for a distribution from the plan account.
  - » Requiring additional validation for distributions (other than a rollover) of the entire balance of the participant's account.
- Procedures for evaluating or testing the security of externally developed applications including periodic reviews and updates.
- A vulnerability management plan, including regular vulnerability scans.
- Annual penetration tests, particularly with respect to customer-facing applications.

9. A Business Resiliency Program which Effectively Addresses Business Continuity, Disaster Recover, and Incident Response.

Business resilience is the ability an organization has to quickly adapt to disruptions while maintaining continuous business operations and safeguarding people, assets, and data. The core components of a program include the Business Continuity Plan, Disaster Recovery Plan, and Incident Response Plan.

- The Business Continuity Plan is the written set of procedures an organization follows to recover, resume, and maintain business functions and their underlying processes at acceptable predefined levels following a disruption.
- The Disaster Recovery Plan is the documented process to recover and resume an organization's IT infrastructure, business applications, and data services in the event of a major disruption.
- The Incident Response Plan is a set of instructions to help IT staff detect, respond to, and recover from security incidents.

An effective Business Resiliency Program should:

- Reasonably define the internal processes for responding to a cybersecurity event or disaster.
- Reasonably define plan goals.
- Define the documentation and reporting requirements regarding cybersecurity events and responses.
- Clearly define and describe the roles, responsibilities, and authority levels.
- Describe external and internal communications and information sharing, including protocols to notify plan sponsor and affected user(s) if needed.
- Identify remediation plans for any identified weaknesses in information systems.
- Include after action reports that discuss how plans will be evaluated and updated following a cybersecurity event or disaster.
- Be annually tested based on possible risk scenarios.

10. Encryption of Sensitive Data Stored and in Transit.

Data encryption can protect nonpublic information. A system should implement current, prudent standards for encryption keys, message authentication and hashing to protect the confidentiality and integrity of the data at rest or in transit.

11. Strong Technical Controls Implementing Best Security Practices.

Technical security solutions are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system. Best security practices for technical security include:

- Hardware, software and firmware models and versions that are kept up to date.
- Vendor-supported firewalls, intrusion detection and prevention appliances/tools.
- Current and regularly updated antivirus software.
- Routine patch management (preferably automated).
- Network segregation.
- System hardening.
- Routine data backup (preferably automated).

12. Responsiveness to Cybersecurity Incidents or Breaches

When a cybersecurity breach or incident occurs, appropriate action should be taken to protect the plan and its participants, including:

- Informing law enforcement.
- Notifying the appropriate insurer.
- Investigating the incident.
- Giving affected plans and participants the information necessary to prevent/reduce injury.
- Honoring any contractual or legal obligations with respect to the breach, including complying with agreed upon notification requirements.
- Fixing the problems that caused the breach to prevent its recurrence.

Cybersecurity Best Practices

On April 14, 2021, the U.S. Department of Labor (DOL) published new guidance for plan sponsors, plan fiduciaries, record keepers and plan participants on best practices for maintaining cybersecurity, including tips on how to protect the retirement benefits of America's workers. The DOL included a list of information security best practices for plan service providers, such as Voya to protect plan participant data. Included in the guidance are *Tips for Hiring a Service Provider with Strong Cybersecurity Practices, Cybersecurity Program Best Practices, and Online Security Tips for Participants and Beneficiaries.*

Voya's information security program has been built on a foundation using industry-recognized best practices and information security frameworks and is aligned to the same core security standards highlighted in the DOL guidance. Voya is committed to protecting the security and confidentiality of the personal information entrusted to us by our customers, and we invest considerable time, effort and resources to safeguard our systems.

Voya's client service contracts are supplemented by a Data Security Addendum, which sets forth Voya's information security practices. The following summary describes how Voya currently supports the DOL's cybersecurity best practices:

1. A Formal, Well Documented Cybersecurity Program.

Yes, Voya has a formal, well-documented cybersecurity program designed to safeguard its infrastructure, information systems and the information in the systems from unauthorized access, use, or other malicious acts.

Voya has implemented and maintains written policies and procedures that address the following:

- access controls and identity management, including required uses for multi-factor authentication;
- asset management;
- business continuity and disaster recovery planning and resources;
- capacity and performance planning;
- configuration management;
- customer data privacy;
- data governance and classification;
- data retention and disposal;
- incident response, including clearly defined roles and decision making authority and a logging and monitoring framework to allow the isolation of an incident.
- maintenance, monitoring and analysis of security audit logs;
- information security;
- physical security and environmental controls;
- risk management;
- system hardening and patch management;
- systems and application development, quality assurance and change management;
- systems and network security, including required uses for encryption to protect sensitive data in transit and at rest; and,
- systems operations and availability concerns;
- vendor and third party service provider management

Voya's information security policies are reviewed annually and have been approved by senior leadership.

2. **Prudent Annual Risk Assessments.**

Yes, Voya conducts prudent annual risk assessments. The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals. The Risk Assessment process overview is provided within Voya's SOC2 Report, which can be provided upon receipt of an executed non-disclosure agreement or pursuant to the client services agreement with Voya.

3. **A Reliable Annual Third Party Audit of Security Controls.**

Yes, Voya has implemented and maintains a reliable annual third party audit of security controls. Voya conducts recurring policy compliance audits by the Internal Corporate Audit Advisory Services team throughout the year. This includes external financial, SOC-1, SOC-2 on the Security Principle and SOX audits on an annual basis, and/or Information Security and Operational Risk Personnel audits throughout the year on an ad hoc basis.

The most recent Service Organization Control 1 (SOC 1) and Service Organization Control 2 (SOC 2) reports will be provided upon request and upon receipt of an executed non-disclosure agreement or pursuant to the services agreement.

At least once every 12 months, Voya engages an external third party to conduct a penetration test of its network. Upon request and pursuant to the services agreement, Voya will provide to Client an executive summary of any material issues or vulnerabilities identified by the most recent Valid Penetration Test along with the scope of systems tested. The report may be redacted to ensure confidentiality.

4. **Clearly Defined and Assigned Information Security Roles and Responsibilities.**

Yes, Voya has clearly defined and assigned information security roles and responsibilities. Voya has designated a qualified employee to serve as its Chief Information Security Officer (“CISO”). The CISO is responsible for overseeing the operations of Voya’s cybersecurity program and enforcing its information security policies. Voya employs experienced and credentialed personnel to manage Voya’s information security risks and perform the core cybersecurity functions of identify, protect, detect, respond and recover. These qualified individuals, who have completed background checks, receive regular updates and training to maintain knowledge of current cybersecurity risks and of changing cybersecurity threats and countermeasures.

5. **Strong Access Control Procedures.**

Yes, Voya has strong access control procedures. Voya implemented and maintains identity management systems and authentication processes for all systems that access, process, store, or transmit customer personal information.

Voya maintains the following user access controls:

- Access to systems that access, process, store, or transmit customer personal information is limited to only those personnel who have been specifically authorized to have access in accordance with the users’ assigned job responsibilities.
- Access to applications and systems is limited to a need-to-know basis, and is enforced through role-based access controls.
- Accounts are reviewed on a periodic and regular basis to ensure that the account is still required, access is appropriate, and the account is assigned to the appropriate user.

- All employees use unique, complex passwords.
- Multi-factor authentication is implemented for all remote access to Voya's internal networks.
- Security event monitoring process and associated mechanisms are in place to ensure events on computing systems, networks, and applications that can impact the security level of that asset or the data residing therein are detected in as close to real-time as possible for those assets used to access, process, store, or transmit customer personal information.

6. Assets or Data Stored in a Cloud or Managed by a Third Party Service Provider are Subject to Appropriate Security Reviews and Independent Security Assessments.

Yes, Voya ensures that any assets or data stored in a cloud or managed by a third party service provider are subject to appropriate security reviews and independent security assessments. Voya has implemented and maintains policies and procedures to ensure the security of personal information and related systems that are accessible to, or held by, third party service providers. Voya does not allow any third parties to access Voya's systems or store or process sensitive data, unless such third parties have entered into written contracts with Voya that require, at a minimum, the following:

- the use of encryption to protect sensitive personal information in transit, and the use of encryption or other mitigating controls to protect sensitive personal information at rest;
- access control policies and procedures, including the use of multi-factor authentication where applicable.
- prompt notice to be provided in the event of a cyber-security incident which directly impacts a customer's information system or non-public personal information;
- the ability of Voya or its agents to perform information security assessments; and
- representations and warranties concerning adequate information security.

7. Cybersecurity Awareness Training Conducted at Least Annually for All Personnel and Updated to Reflect Risks Identified by the Most Recent Risk Assessment.

Yes, Voya conducts annual cybersecurity awareness training for all personnel and updates the training to reflect risks identified by the most recent risk assessment. Voya provides regular information security and privacy education and training to all Voya Personnel, as relevant for their job function. In addition, Voya provides targeted training to information security personnel and requires key information security personnel to stay abreast of changing cybersecurity threats and countermeasures.

8. Secure System Development Life Cycle Program (SDLC).

Yes, Voya has implemented and manages a secure system development life cycle (SDLC) program. Voya has a formal SDLC process that includes peer code review, integration testing, and acceptance testing, all of which have built-in security processes. Voya maintains physically and/or logically separate development, test, and production computing environments.

Voya implements and maintains an application security certification and assurance process that ensures that all applications that access, process, store, or transmit customer personal information provide the following:

- Application and database design ensures security, accuracy, completeness, timeliness, and authentication/authorization of inputs, processing, and outputs.

- All data inputs are validated for invalid characters, out of range values, invalid command sequences, exceeding data limits, etc. prior to being accepted for production. Voya implements static source code analysis tools to validate data inputs.
- Application source code developed in house by Voya is protected through the use of a source code repository that ensures version and access control. The version management system provides segregation of code, data and environments.
- Applications and databases are tested for security robustness and corrective measures are applied prior to the application being placed into a production environment. All systems are configured to meet Voya standards, monitored to ensure compliance state, and patched as required to maintain a high degree ofsecurity.
- Voya implements and maintains vulnerability and penetration testing (Ethical Hacking) processes to ensure the computing environment where customer personal information is accessed, processed, stored, or transmitted is continually protected from internal and external security threats

9. A Business Resiliency Program which Effectively Addresses Business Continuity, Disaster Recovery, and Incident Response.

Yes, Voya has an effective business resiliency program that addresses business continuity, disaster recovery, and incident response. As part of its business resiliency program, Voya maintains the following:

- a written business continuity plan (BCP) that permits Voya to recover from a disaster and continue providing services to customers within the recovery time objectives set forth in the BCP;
- a written disaster recovery plan designed to maintain customer access to services and prevent the unintended loss or destruction of customer data; and
- an incident response process to ensure that all events with a potential security impact are identified, investigated, contained, remediated, and reported to the client effectively and in a timely manner.

10. Encryption of Sensitive Data Stored and in Transit.

Yes, Voya encrypts sensitive data stored and in transit. Voya implemented and maintains cryptographic controls for the protection of personal information, including the following:

- use of an encryption standard equal to or better than the industry standards included in applicable National Institute for Standards and Technology Special Publications (or such higher encryption standard required by applicable Law) to protect personal information at rest and in transit over un-trusted networks;
- use of cryptographic techniques to provide evidence of the occurrence or nonoccurrence of an event or action;
- use of cryptographic techniques to authenticate users and other system entities requesting access to or transacting with system users, entities and resources; and
- development and implementation of policies on the use, protection and lifetime of cryptographic keys through their entire lifecycle.

11. Strong Technical Controls Implementing Best Security Practices.

Yes, Voya implemented strong technical controls in accordance with best security practices. Voya established and maintains:

- administrative, technical, and physical safeguards against the destruction, loss, or alteration of Personal Information; and
- appropriate security measures to protect personal information, which measures meet or exceed the requirements of all applicable Laws relating to personal information security.

In addition, Voya implemented and maintains the following information security controls:

- restricted and controlled privileged access rights;
- an inventory of assets relevant to the lifecycle of information;
- network security controls, including firewall and intrusion prevention services;
- detection, prevention and recovery controls to protect against malware, including current and regularly updated antivirus software;
- systems are configured to meet Voya standards, monitored to ensure a compliant state, and patched as required to maintain a high degree of security.
- information about technical vulnerabilities of Voya's information systems is obtained and evaluated in a timely fashion and appropriate measures taken to address the risk;
- protected storage and storage systems;
- detailed event logs recording user activities, exceptions, faults, access attempts, operating system logs, and information security events are produced, retained and regularly reviewed as needed; and
- separated development, testing and operational environments to reduce the risks of unauthorized access or changes to the operational environment.

12. Responsiveness to Cybersecurity Incidents or Breaches.

Yes, Voya takes appropriate action to protect its clients upon a cybersecurity incident or breach. Voya is committed to protecting the security and privacy of the personal information entrusted to us by our customers, and we invest considerable time, effort and resources to protect our systems. As part of this commitment, Voya established a formal Cyber Fusion Threat Center (CFTC) with responsibility to proactively detect and analyze threats to information assets within the Voya enterprise, including communication and escalation of information security events to Voya's Security Incident Response team. The CFTC leverages threat intelligence feeds from multiple sources and takes immediate action as necessary.

Voya implemented and maintains an incident management process to ensure that all events with a potential security impact are identified, investigated, contained, remediated, and reported to the client effectively and in a timely manner. In the event a cybersecurity incident occurs, Voya complies with all notification obligations under applicable state and federal laws and regulations.

TIAA Cybersecurity – An Overview of Our Alignment to the DOL's Cybersecurity Guidelines

In April 2021, the United States Department of Labor (DOL) released cybersecurity guidelines that detail best practices for cybersecurity program management, tips for hiring a retirement plan service provider with strong cybersecurity practices, and online security tips for plan participants. The DOL's guidelines were issued in response to a March 2021 report from the Government Accountability Office (GAO) titled *Federal Guidance Could Help Mitigate Cybersecurity Risks in 401(k) and Other Retirement Plans*.

TIAA fully supports both the GAO and the DOL for thoroughly addressing a topic of such great importance. We have long made cybersecurity and the protection of participant, plan and financial information a top priority and our processes are aligned and compliant with the DOL guidelines.

The second piece of guidance, *Cybersecurity Program Best Practices*, details best practices for maintaining a strong cybersecurity defense. In addition to providing a framework for recordkeepers and other service providers responsible for plan-related IT systems and data, these tips and best practices are a valuable reference for retirement plan fiduciaries when evaluating the cybersecurity practices of service providers.

The following is a summary of TIAA's current controls and practices aligned with the DOL's recommended best practices.

1. Have a formal, well-documented cybersecurity program.

Teachers Insurance and Annuity Association of America (also "TIAA") has a formal, well-documented cybersecurity program. TIAA is an insurance company regulated by the New York Department of Financial Services, as well as a savings and loan holding company subject to the oversight of the Federal Reserve Bank of Boston. As such, TIAA is required to maintain a written, risk-based cybersecurity program ("Cybersecurity Program") pursuant to the Gramm Leach Bliley Act of 1999 ("GLBA"), the Fair Credit Reporting Act ("FCRA") as amended by the Fair and Accurate Credit Transactions Act of 2003 ("FACT Act"), the respective regulations promulgated thereunder, including the Federal Financial Institutions Examination Council (FFIEC) Examination Guidance and the NY DFS Cybersecurity Regulation, and applicable state privacy laws, including but not limited to 201 CMR 17.00 et. seq. Our Cybersecurity Program is also mapped against the International Organization for Standardization/the International Electrotechnical Commission (ISO/IEC 27002) and the National Institute of Standards and Technology (NIST) Cybersecurity Framework and is consistent with the DOL's "Cybersecurity Program Best Practices."

Within TIAA's Cybersecurity Program, the privacy and security of our clients' information is the top priority. TIAA combines technology, people, and process to protect client data and to identify, prevent, defend against, and respond to anticipated threats. TIAA's Cybersecurity Program is documented in enterprise policies, control standards, and standard operating procedures that reflect the procedural aspects of operations.

The policies, standards, and operational components of our Cybersecurity Program are regularly reviewed by internal stakeholders, assessed by internal and external auditors, and examined by regulators.

For more information, please see the following resources:

TIAA.org Security Center

Cybersecurity Program Overview

TIAA Alignment to DOL Guidelines

Cybersecurity Insights Article – What you don't know can hurt you

2. Conduct prudent annual risk assessments.

TIAA operates a robust enterprise risk management framework with explicit first, second, and third lines of defense. Cybersecurity operates within that risk framework and performs detailed risk assessments on TIAA's Information Technology ("IT") assets (including, but not limited to, business applications, servers, databases, network devices, end user devices, and suppliers). Risk classification occurs at least annually, and subsequent control assessments are performed with varied frequency based on inherent risk ratings. Emerging risks and technologies are also consistently evaluated, and new assessment capabilities are developed and put into operation as needed.

Risk assessment details are formally documented and any findings are reviewed in accordance with TIAA's enterprise risk management framework and managed accordingly.

Within the enterprise risk management framework, TIAA additionally conducts various vulnerability assessments and employs external parties to perform targeted penetration and vulnerability assessments against our systems and networks. TIAA regularly updates its computing environment with security vulnerability patches and other similar safeguards to address identified risks.

3. Have a reliable annual third-party audit of security controls.

TIAA's Cybersecurity Program is risk-based, consistent with regulatory obligations and examination guidance applicable to financial institutions, industry standards and the DOL guidance. This risk-based approach requires the adoption, implementation and review of controls to minimize risks to customer information and includes the Federal Financial Institutions Examination Council (FFIEC) booklets, International Organization for Standardization/the International Electrotechnical Commission (ISO/IEC 27002), National Institute of Standards and Technology (NIST), as applicable.

TIAA is regularly assessed by internal and external auditors, and engages a nationally recognized accounting firm to issue Statement on Standards for Attestation Engagements No. 18 (SSAE18) (formerly SSAE16, SAS70) SOC1 and SOC2 reports for Defined Contribution Retirement Recordkeeping annually.

The reports include a transparent view of TIAA's business operations, as well as our cybersecurity, and IT availability controls.

With regards to cybersecurity, the most recent SOC2 covers the period of 1/1/2020 to 12/31/2020 and was "unmodified." TIAA is happy to provide its SOC2 results to clients, upon request.

4. Clearly define and assign information security roles and responsibilities.

TIAA's management, in particular the Board of Directors and Senior Executive Management, is responsible for overseeing the execution and delivery of TIAA's Cybersecurity Program through TIAA's Chief Information Security Officer (CISO). The CISO role is a dedicated executive position with principal responsibility for overseeing TIAA's Cybersecurity Program as dictated in TIAA's IT policies, standards, and operating procedures. TIAA's current CISO's background includes more than 15 years of information security experience in the financial services sector and includes numerous executive positions. He is also an active board member of The Financial Services Information Sharing and Analysis Center (FS-ISAC) and the chairperson of the Information Security Committee of BITs (a division of the Bank Policy Institute).

The CISO also chairs TIAA's Information Security Leadership Committee (ISLC) which has been established with representation from Technology, Legal, Operations Risk, Compliance, Business Operations, Internal Audit, and others to:

- Create enterprise strategic planning for security priorities
- Recommend and approve IT policies and standards for enterprise adoption
- Ensure cross-functional collaboration on all security incidents
- Identify, select and adapt controls based on identified threats, risks and cost-benefit analysis
- Provide guidance and leadership for protecting information from unauthorized access, destruction, modification, and disclosure
- Initiate and monitor associated risk action plans, progress against plans, and supporting performance and operational metrics
- Leverage and implement IT risk best practices across all business areas
- Coordinate corporate security initiatives at the senior leader level
- Ensure representation from all business areas to provide a firm-wide approach to information security

5. Have strong access control procedures.

TIAA's Cybersecurity Program maintains a comprehensive identity and access management program that provides oversight on the following related controls for TIAA's workforce:

- Systems access and entitlements are granted on a need-to-know basis. Only the minimum level of access required for successful job completion is permitted.
- Systems access and entitlements are reviewed by management on a recurring basis and revoked when job functions change or upon separation from TIAA. Initial access and entitlements are only provisioned with appropriate management approvals.
- Password requirements are based on industry best practices and passwords require reset with a recurring frequency.

- Multi-factor authentication is required to access TIAA's network.
- TIAA's participant websites implement risk-based adaptive multi-factor authentication to secure user authentication and sensitive transactions; users can elect to always use a one-time PIN or biometrics (on TIAA's mobile app and IVR) to authenticate.

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

TIAA operates a robust enterprise risk management framework with explicit first, second, and third lines of defense. As part of that framework, TIAA operates an explicit Supplier Risk Management function that oversees initial and recurring risk assessments of suppliers. Suppliers are assessed against TIAA's policies and standards before engagement and risks are documented, classified, and managed. Suppliers are reassessed on a recurring basis.

TIAA's contracts with suppliers address cybersecurity concerns as stated in the DOL guidelines.

7. Conduct periodic cybersecurity awareness training.

TIAA operates an enterprise-wide cybersecurity training and awareness program that drives a culture of security accountability across TIAA's workforce. The program aims to ensure TIAA's workforce understands comprehensive security is the responsibility of every employee at TIAA, and not just the responsibility of cybersecurity professionals or technological controls. TIAA's workforce is educated to recognize attack vectors, maintain vigilance, and employees understand how to report any potential threats.

TIAA's workforce is required to complete formal risk management and cybersecurity training upon joining the company and also on a recurring basis. TIAA further provides targeted online training to certain employees based on their role or at-risk behaviors. Examples of this more targeted formal training can include extensive training on secure coding for employees operating in software development roles and specialized training for privileged users. Training completion is monitored, recorded and reported to management.

TIAA also conducts recurring phishing email simulations across TIAA's workforce. Phishing continues to be an effective attack vector for malicious parties, and this program drives vigilance and accountability around these dangers. Phishing simulation results are reported to TIAA's Board of Directors to ensure proper visibility and oversight. TIAA additionally sponsors recurring cybersecurity-related enterprise communications and enterprise-wide events that remind employees of their security responsibilities.

Within TIAA's Cybersecurity Program, TIAA further ensures its cybersecurity workforce undergoes continuous training on security tools, emerging threats and cybersecurity concepts. TIAA has a strong academic relationship with New York University (NYU) and has a significant number of employees pursuing cyber-related graduate degrees at the school, the most of any of NYU's current industry partners. To recognize this outstanding commitment to cybersecurity education, TIAA was awarded a CSO50 Award in early 2021.

For more information, please see the following resource:

TIAA Cybersecurity Earns Top Honor for focus on academics

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

TIAA's software development teams adhere to a policy-based secure systems development life cycle (SDLC) methodology to manage software development and ongoing systems maintenance. This methodology, and associated governance activities, ensure proper software development procedures. These procedures include, but are not limited to, planning, analysis, design, development, testing, and user documentation, and further include analysis, design, implementation, and testing of security requirements. Using a risk-based approach, the methodology requires software development teams to collaborate with Cybersecurity Architects and cybersecurity subject matter experts to help ensure security policy and standards are included. Developers additionally deploy integrated vulnerability scanning tools and use a risk-based approach to remediate findings accordingly. Developers are required to undergo formal training on secure coding and tools.

TIAA's policies and standards dictate security features and functionality that must be included in appropriate transaction-based software to ensure alerts, logging, and additional user validation (i.e., multi-factor authentication for certain transactions) are in place, per regulatory guidance. As part of TIAA's enterprise risk management framework, business applications (regardless of source or hosting) are assessed for risk against all applicable policies and standards on a recurring basis.

TIAA additionally conducts network, host, and application vulnerability and risk assessments, and employs external parties to perform targeted penetration and vulnerability assessments against systems and networks. TIAA regularly updates its computing environment with security vulnerability patches and other similar safeguards to address identified risks.

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

TIAA has well-documented business continuity and disaster recovery programs and plans that are regularly reviewed and tested. Business-critical functions are required to have procedures in place to make sure business operations can continue in an emergency. TIAA's business continuity plan covers operational criteria including, but not limited to:

- Backing up and recovering data
- Building redundancy into all critical systems
- Maintaining geographically diverse business center locations, personnel, processes and technology
- Minimizing financial, operational and credit risk exposures
- Establishing alternate ways to communicate with our participants
- Confirming emergency contacts and alternate business facilities for our employees
- Arranging emergency procedures with critical business partners, such as banks
- Communicating with and reporting to regulators
- Ensuring participants have prompt access to their accounts and funds

10. Encrypt sensitive data, stored and in transit.

TIAA's Cybersecurity Program implements a comprehensive data loss prevention program that defines data classification parameters, educates TIAA's workforce on those parameters, provides tools to support data classification efforts, and implements numerous controls to reduce the risk of any unauthorized data exposure. These controls include, but are not limited to, encryption of sensitive data in storage, encryption of sensitive data in transit, encryption of portable employee devices, and network monitoring.

The controls implemented by TIAA's data loss prevention program are dictated by TIAA's IT policies and standards.

11. Implement strong technical controls in accordance with best security practices.

TIAA's Cybersecurity Program implements numerous layers of comprehensive technologies to prevent, detect, and respond to malicious activity and to protect client data and company assets from anticipated threats. TIAA implements the latest in firewall, intrusion prevention, antivirus, backup, and other technologies. Recurring scanning is conducted to identify vulnerabilities in hardware, software, and firmware models, and versions and stringent patching requirements are enforced, monitored, and reported to management.

12. Appropriately respond to cybersecurity incidents.

TIAA implements and maintains a multi-disciplinary, enterprise-wide incident response program based on the banking regulators' "Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice." In the event of an incident or breach, there are procedures in place to investigate, contain, and mitigate the impact and risk to clients and the enterprise, as well as to restore capabilities or services that were impacted. As part of our incident response plan, if there was a breach of customer data, TIAA follows all applicable state and federal regulations regarding notification of affected individuals and regulators; TIAA also offers affected individuals two years' credit monitoring, ID theft repair and ID theft insurance, at TIAA's sole cost and expense.