AGREEMENT

THIS AGREEMENT is made and entered into this 25th day of February, 2020, by and between the COUNTY OF FRESNO, a Political Subdivision of the State of California, hereinafter referred to as "COUNTY", and ReliaStar Life Insurance Company, a Minnesota Corporation, whose address is 20 Washington Ave. S., Minneapolis, MN 55401, hereinafter referred to as "CONTRACTOR".

WITNESSETH:

WHEREAS, the County of Fresno desires to provide optional, voluntary Accident, Critical Illness and Hospital Indemnity Insurance coverage to its employees; and

WHEREAS, Department of Human Resources staff solicited bids for Insurance rates from qualified vendors; and

WHEREAS, CONTRACTOR submitted the most responsive bid for such Insurance services;

NOW, THEREFORE, in consideration of the mutual covenants, terms and conditions herein contained, the parties hereto agree as follows:

1. OBLIGATIONS OF THE CONTRACTOR

A. CONTRACTOR shall provide to eligible COUNTY employees, their spouses and/or children who opt to purchase such insurance, Compass Accident Insurance, Compass Critical Illness Insurance, and Compass Hospital Confinement Indemnity Insurance as described in Exhibit A, attached hereto and incorporated herein by this reference. Premiums for this optional insurance will be paid by the covered employee, through payroll deductions, and will not be paid by the COUNTY.

B. Eligibility. All permanent employees of COUNTY who work twenty (20) or more hours per week are eligible for coverage. Employees may also elect coverage for their spouses and/or children, provided that the employee elects coverage for themselves.

2. OBLIGATIONS OF THE COUNTY

A. Policy Administration. COUNTY will maintain all enrollment, beneficiary, and billing records for the Policies (as applicable), including the following:

1) appropriately apply Policy limits and rules

2) know how much coverage the employee has at all times

3) provide the employee with the appropriate “Conversion” and/or “Portability” documentation (as applicable)

4) set up any payroll deductions correctly

5) pay premium to the insurance company with supporting documentation

6) file a claim

B. Evidence of Insurability. If evidence of insurability is required in connection with an application for coverage under the terms of a Policy, COUNTY will apply the evidence of insurability rules appropriately, obtain the necessary forms from any applicant for such coverage and provide those forms to the CONTRACTOR.

C. Claim Administration. Upon receipt of notice of a potential claim under a Policy, COUNTY will confirm employees’ eligibility for coverage and provide required claim documentation at CONTRACTOR’S request. CONTRACTOR shall be responsible for all claim reviews, determinations and payments.

D. Record Keeping. COUNTY shall maintain accurate books and records documenting the administration of the Policies, including employee demographics, eligibility records, dependent data, coverage amounts, enrollment history, payroll deductions, benefit elections and beneficiary designations (as applicable).

3. TERM

The term of this Agreement shall be for a period of three (3) years, commencing on May 1, 2020, through and including April 30, 2023.

4. TERMINATION

A. Non-Allocation of Funds - The terms of this Agreement, and the services to be provided hereunder and in accordance with the issued insurance policies, are contingent on the approval of funds by the appropriating government agency. Should sufficient funds not be allocated, the services provided may be modified, or this Agreement terminated, at any time by giving the CONTRACTOR thirty-one (31) days advance written notice.

B. Breach of Contract - The COUNTY may immediately suspend or terminate this Agreement in whole or in part, where in the determination of the COUNTY there is:

1) An illegal or improper use of funds;

2) A failure to comply with any term of this Agreement;

3) A substantially incorrect or incomplete report submitted to the COUNTY;

4) Improperly performed service.

In no event shall any payment by the COUNTY constitute a waiver by the COUNTY of any breach of this Agreement or any default which may then exist on the part of the CONTRACTOR. Neither shall such payment impair or prejudice any remedy available to the COUNTY with respect to the breach or default.

C. Without Cause - Under circumstances other than those set forth above, this Agreement may be terminated by COUNTY upon the giving of thirty-one (31) days advance written notice of an intention to terminate to CONTRACTOR.

5. COMPENSATION & INVOICING: Eligible COUNTY employees who opt to purchase insurance provided by CONTRACTOR under this Agreement shall pay the following premiums:

A. Critical Illness Insurance. Employees and their spouse and/or eligible children who choose to enroll in a Critical Illness Insurance policy are subject to the following monthly rates per $1,000 of coverage, based on their age:

1) Under 30 years of age: $0.26

2) 30-39 years of age: $0.35

3) 40-49 years of age: $0.78

4) 50-59 years of age: $1.92

5) 60-64 years of age: $3.17

6) 65-69 years of age: $4.27

7) 70 years of age or older: $6.58

8) All children of the employee: $0.28

B. Hospital Indemnity Insurance. Employees and their spouse and/or eligible children who choose to enroll in a Critical Illness Insurance policy are subject to the following monthly rates:

1) Employee Only, $100 daily benefit: $10.45

2) Employee & Spouse, $100 daily benefit: $20.70

3) Employee & Children, $100 daily benefit: $16.24

4) Family, $100 daily benefit: $26.49

5) Employee Only, $200 daily benefit: $23.40

6) Employee & Spouse, $200 daily benefit: $46.33

7) Employee & Children, $200 daily benefit: $35.82

8) Family, $200 daily benefit: $58.75

C. Accident Insurance. Employees and their spouse and/or eligible children who choose to enroll in an Accident Insurance policy are subject to the following monthly rates:

1) Employee Only, Low Plan: $4.73

2) Employee & Spouse, Low Plan: $8.95

3) Employee & Children, Low Plan: $9.15

4) Family, Low Plan: $13.37

5) Employee Only, High Plan: $7.16

6) Employee & Spouse, High Plan: $12.90

7) Employee & Children, High Plan: $14.49

8) Family, High Plan: $20.23

There is no cost to COUNTY for services performed under this Agreement. It is understood that all expenses incidental to CONTRACTOR'S performance of services under this Agreement shall be borne by CONTRACTOR. Premiums will be deducted by COUNTY semi-monthly from participating employees' paychecks and shall be remitted by COUNTY to CONTRACTOR no sooner than 45 days after the last calendar day of the month in which premiums are collected.

6. INDEPENDENT CONTRACTOR: In performance of the work, duties and obligations assumed by CONTRACTOR under this Agreement, it is mutually understood and agreed that CONTRACTOR, including any and all of the CONTRACTOR'S officers, agents, and employees will at all times be acting and performing as an independent contractor, and shall act in an independent capacity and not as an officer, agent, servant, employee, joint venturer, partner, or associate of the COUNTY. Furthermore, COUNTY shall have no right to control or supervise or direct the manner or method by which CONTRACTOR shall perform its work and function. However, COUNTY shall retain the right to administer this Agreement so as to verify that CONTRACTOR is performing its obligations in accordance with the

terms and conditions thereof.

CONTRACTOR and COUNTY shall comply with all applicable provisions of law and the rules and regulations, if any, of governmental authorities having jurisdiction over matters the subject thereof.

Because of its status as an independent contractor, CONTRACTOR shall have absolutely no right to employment rights and benefits available to COUNTY employees. CONTRACTOR shall be solely liable and responsible for providing to, or on behalf of, its employees all legally-required employee benefits. In addition, CONTRACTOR shall be solely responsible and save COUNTY harmless from all matters relating to payment of CONTRACTOR'S employees, including compliance with Social Security withholding and all other regulations governing such matters. It is acknowledged that during the term of this Agreement, CONTRACTOR may be providing services to others unrelated to the COUNTY or to this Agreement.

7. PROTECTED HEALTH INFORMATION

A. The parties to this Agreement shall be in strict conformance with all applicable Federal and State of California laws and regulations, as well as the Protected Health Information Confidentiality Agreement, attached hereto as Exhibit B and incorporated herein by this reference.

B. Safeguards

CONTRACTOR shall implement administrative, physical, and technical safeguards as required by applicable law and as further described in the provisions of Exhibit C “Data Security Agreement,” attached hereto and incorporated herein by this reference.

C. Survival

The respective rights and obligations of the parties as stated in this Section shall survive the termination or expiration of this Agreement.

D. No Waiver of Obligations

No change, waiver or discharge of any liability or obligation hereunder on any one or more occasions shall be deemed a waiver of performance of any continuing or other obligation, or shall prohibit enforcement of any obligation on any other occasion.

8. MODIFICATION: Any matters of this Agreement may be modified from time to time by the written consent of all the parties without, in any way, affecting the remainder.

9. NON-ASSIGNMENT: Neither party shall assign, transfer or sub-contract this Agreement

nor their rights or duties under this Agreement without the prior written consent of the other party. Notwithstanding the foregoing, COUNTY or CONTRACTOR may subcontract certain administrative services in the performance of its obligations under this Agreement.

10. HOLD HARMLESS: CONTRACTOR agrees to indemnify, save, hold harmless, and at COUNTY'S request, defend the COUNTY, its officers, agents, and employees from any and all costs and expenses (including attorney's fees and costs), damages, liabilities, claims, and losses occurring or resulting to COUNTY in connection with any error or omission, by CONTRACTOR, its officers, agents, or employees under this Agreement, and from any and all costs and expenses (including attorney's fees and costs), damages, liabilities, claims, and losses occurring or resulting to any person, firm, or corporation who may be injured or damaged by any error or omission, of CONTRACTOR, its officers, agents, or employees under this Agreement, except to the extent COUNTY has caused or significantly contributed to the error or omission.

11. INSURANCE:

Without limiting the COUNTY's right to obtain indemnification from CONTRACTOR or any third parties, CONTRACTOR, at its sole expense, shall maintain in full force and effect, the following insurance policies or a program of self-insurance, including but not limited to, an insurance pooling arrangement or Joint Powers Agreement (JPA) throughout the term of the Agreement:

A. Commercial General Liability

Commercial General Liability Insurance with limits of not less than Two Million Dollars ($2,000,000.00) per occurrence and an annual aggregate of Four Million Dollars ($4,000,000.00). This policy shall be issued on a per occurrence basis. COUNTY may require specific coverages including completed operations, products liability, contractual liability, Explosion-Collapse-Underground, fire legal liability or any other liability insurance deemed necessary because of the nature of this contract.

B. Automobile Liability

Comprehensive Automobile Liability Insurance with limits of not less than One Million Dollars ($1,000,000.00) per accident for bodily injury and for property damages. Coverage should include any auto used in connection with this Agreement.

C. Professional Liability

If CONTRACTOR employs licensed professional staff, (e.g., Ph.D., R.N., L.C.S.W., M.F.C.C.) in providing services, Professional Liability Insurance with limits of not less than One Million Dollars ($1,000,000.00) per occurrence, Three Million Dollars ($3,000,000.00) annual aggregate.

D. Worker's Compensation

A policy of Worker's Compensation insurance as may be required by the California Labor Code.

E. Cyber Liability

Cyber Liability Insurance, with limits not less than $2,000,000 per occurrence or claim, $2,000,000 aggregate. Coverage shall be sufficiently broad to respond to the duties and obligations as is undertaken by Vendor in this agreement and shall include, but not be limited to, claims involving infringement of intellectual property, including but not limited to infringement of copyright, trademark, trade dress, invasion of privacy violations, information theft, damage to or destruction of electronic information, release of private information, alteration of electronic information, extortion and network security. The policy shall provide coverage for breach response costs as well as regulatory fines and penalties as well as credit monitoring expenses with limits sufficient to respond to these obligations.

F. Technology Professional Liability (Errors and Omissions)

Technology Professional Liability (Errors and Omissions) Insurance appropriate to the CONTRACTOR's profession, with limits not less than $2,000,000 per occurrence or claim, $2,000,000 aggregate. Coverage shall be sufficiently broad to respond to the duties and obligations as is undertaken by CONTRACTOR in this agreement and shall include, but not be limited to, claims involving infringement of intellectual property, including but not limited to infringement of copyright, trademark, trade dress, invasion of privacy violations, information theft, damage to or destruction of electronic information, release of private information, alteration of electronic information, extortion and network security. The policy shall provide coverage for breach response costs as well as regulatory fines and penalties as well as credit monitoring expenses with limits sufficient to respond to these obligations.

Additional Requirements Relating to CONTRACTOR's Professional Liability Insurance

CONTRACTOR shall obtain endorsements to the Commercial General Liability insurance naming the County of Fresno, its officers, agents, and employees, individually and collectively, as additional

insured, but only insofar as the operations under this Agreement are concerned. Such coverage for additional insured shall apply as primary insurance and any other insurance, or self-insurance, maintained by COUNTY, its officers, agents and employees shall be excess only and not contributing with insurance provided under CONTRACTOR's policies herein. This insurance shall not be cancelled or changed without a minimum of thirty (30) days advance written notice given to COUNTY.

CONTRACTOR hereby waives its right to recover from COUNTY, its officers, agents, and employees any amounts paid by the policy of worker's compensation insurance required by this Agreement. CONTRACTOR is solely responsible to obtain any endorsement to such policy that may be necessary to accomplish such waiver of subrogation, but CONTRACTOR's waiver of subrogation under this paragraph is effective whether or not CONTRACTOR obtains such an endorsement.

Within Thirty (30) days from the date CONTRACTOR signs and executes this Agreement, CONTRACTOR shall provide certificates of insurance and endorsement as stated above for all of the foregoing policies, as required herein, to the County of Fresno, Paul Nerland, Director of Human Resources, 2220 Tulare Street, 14th Floor, Fresno, CA 93721, stating that such insurance coverage have been obtained and are in full force; that the County of Fresno, its officers, agents and employees will not be responsible for any premiums on the CONTRACTOR's professional liability policies; that for such worker's compensation insurance the CONTRACTOR has waived its right to recover from the COUNTY, its officer, agents, and employees any amounts paid under the insurance policy and that waiver does not invalidate the insurance policy; that such Commercial General Liability insurance names the County of Fresno, its officers, agents and employees, individually and collectively, as additional insured, but only insofar as the operations under this Agreement are concerned; that such coverage for additional insured shall apply as primary insurance and any other insurance, or self-insurance, maintained by COUNTY, its officers, agents and employees, shall be excess only and not contributing with insurance provided under CONTRACTOR's policies herein; and that this insurance shall not be cancelled or changed without a minimum of thirty (30) days advance, written notice given to COUNTY.

In the event CONTRACTOR fails to keep in effect at all times insurance coverage as herein provided, the COUNTY may, in addition to other remedies it may have, suspend or terminate this Agreement upon the occurrence of such event.

All policies shall be issued by admitted insurers licensed to do business in the State of California, and such insurance shall be purchased from companies possessing a current A.M. Best, Inc. rating of A FSC VII or better.

12. AUDITS AND INSPECTIONS:

The CONTRACTOR shall make available to the COUNTY records and data with respect to the matters covered by this Agreement. The CONTRACTOR shall, upon request by the COUNTY, to occur not more than once annually, permit the COUNTY to audit and inspect all of such relevant records and data necessary to ensure CONTRACTOR'S compliance with the terms of this Agreement. For the avoidance of doubt, such records will be limited to financial and administrative records directly related to the insurance Policies issued to COUNTY and will not include any employee personal health information or other information to which access is limited by applicable law, nor will it include any onsite audits

If this Agreement exceeds ten thousand dollars ($10,000.00), CONTRACTOR shall be subject to the examination and audit of the Auditor General for a period of three (3) years after final payment under contract (Government Code Section 8546.7).

13. NOTICES: The persons and their addresses having authority to give and receive notices under this Agreement include the following:

COUNTY	CONTRACTOR
COUNTY OF FRESNO 2220 Tulare Street, 14th Floor Fresno, CA 93721	ReliaStar Life Insurance Company 20 Washington Ave S. Minneapolis, MN 55401

All notices between the COUNTY and CONTRACTOR provided for or permitted under this Agreement must be in writing and delivered either by personal service, by first-class United States mail, by an overnight commercial courier service, or by telephonic facsimile transmission. A notice delivered by personal service is effective upon service to the recipient. A notice delivered by first-class United States mail is effective three COUNTY business days after deposit in the United States mail, postage prepaid, addressed to the recipient. A notice delivered by an overnight commercial courier service is effective one COUNTY business day after deposit with the overnight commercial courier service, delivery fees prepaid, with delivery instructions given for next day delivery, addressed to the recipient. A notice delivered by telephonic facsimile is effective when transmission to the recipient is completed (but, if such transmission is

completed outside of COUNTY business hours, then such delivery shall be deemed to be effective at the next beginning of a COUNTY business day), provided that the sender maintains a machine record of the completed transmission. For all claims arising out of or related to this Agreement, nothing in this section establishes, waives, or modifies any claims presentation requirements or procedures provided by law, including but not limited to the Government Claims Act (Division 3.6 of Title 1 of the Government Code, beginning with section 810).

14. GOVERNING LAW: Venue for any action arising out of or related to this Agreement shall only be in Fresno County, California.

The rights and obligations of the parties and all interpretation and performance of this Agreement shall be governed in all respects by the laws of the State of California.

15. DISCLOSURE OF SELF-DEALING TRANSACTIONS

This provision is only applicable if the CONTRACTOR is operating as a corporation (a for-profit or non-profit corporation) or if during the term of the agreement, the CONTRACTOR changes its status to operate as a corporation.

Members of the CONTRACTOR's Board of Directors shall disclose any self-dealing transactions that they are a party to while CONTRACTOR is providing goods or performing services under this agreement. A self-dealing transaction shall mean a transaction to which the CONTRACTOR is a party and in which one or more of its directors has a material financial interest. Members of the Board of Directors shall disclose any self-dealing transactions that they are a party to by completing and signing a Self-Dealing Transaction Disclosure Form, attached hereto as Exhibit D and incorporated herein by reference, and submitting it to the COUNTY prior to commencing with the self-dealing transaction or immediately thereafter.

16. ENTIRE AGREEMENT: This Agreement constitutes the entire agreement between the CONTRACTOR and COUNTY with respect to the subject matter hereof and supersedes all previous Agreement negotiations, proposals, commitments, writings, advertisements, publications, and understanding of any nature whatsoever unless expressly included in this Agreement. In the event of any inconsistency in interpreting the documents which constitute this Agreement, the inconsistency shall be resolved by giving precedence in the following order of priority: (1) the text of this Agreement (excluding

Exhibits A, B, and C, (2) Exhibits A, B, and C. Notwithstanding the foregoing, the parties understand and acknowledge that any insurance obligations owed to County or its employee participants will be governed solely by the terms of the insurance policies issued by CONTRACTOR under the terms of this Agreement.

///

///

///

///

///

///

///

///

///

///

///

///

///

///

///

///

///

///

///

///

///

///

///

IN WITNESS WHEREOF, the parties hereto have executed this Agreement as of the day and year first hereinabove written.

CONTRACTOR

Mona Zielke
(Authorized Signature)

Mona Zielke
SVP, Enterprise Claims & EB Operations
Print Name & Title

20 Washington Ave South
Minneapolis, MN 55401
Mailing Address

COUNTY OF FRESNO

Ernest Buddy Mendes, Chairman of the Board of Supervisors of the County of Fresno

ATTEST:
Bernice E. Seidel
Clerk of the Board of Supervisors
County of Fresno, State of California

By: Susan Bishop
Deputy

FOR ACCOUNTING USE ONLY:

ORG No.:
Account No.:
Requisition No.:

EXHIBIT A

Compass Accident Insurance

A Proposal for County of Fresno

Compass Accident Insurance — Benefit schedule (may vary by state)

Accident Hospital Care (in $'s)

	Level 2	Level 4
Surgery (open abdominal, thoracic)	800	1,200
Surgery (exploratory or without repair)	125	175
Blood, Plasma, Platelets	400	600
Hospital Admission	1,000	1,250
Hospital Confinement (per day up to 365 days)	300	375
Critical Care Unit Confinement (per day up to 15 days)	475	600
Rehabilitation Facility Confinement (per day up to 90 days)	125	200
Coma (duration of 14 or more days)	11,500	17,000
Transportation (per trip, up to once per accident)	500	750
Lodging (per day up to 30 days)	120	180
Family care (per child per day up to 45 days)	15	25

A Proposal for County of Fresno

Accident Care (in $'s)

	Level 2	Level 4
Initial Doctor Visit	60	90
Urgent Care Facility Treatment	150	225
Emergency Room Treatment	150	225
Ground Ambulance	240	360
Air Ambulance	1,000	1,500
Follow-Up Doctor Treatment	60	90
Chiropractic Treatment (up to 6 per accident)	30	45
Medical Equipment	40	120
Physical or Occupational Therapy (up to 6 per accident)	30	45
Speech Therapy (up to 6 per accident)	30	45
Prosthetic Device (one)	500	750
Prosthetic Device (two or more)	800	1,200
Major Diagnostic Exams	80	240
Outpatient Surgery (once per accident)	150	225
X-ray	30	45

A Proposal for County of Fresno

Common Injuries (in $'s)

	Level 2	Level 4
Burns (2nd degree, at least 36% of body)	1,000	1,250
Burns (3rd degree, at least 9 but less than 35 sq in of body)	4,500	7,500
Burns (3rd degree, 35 or more sq in of body)	10,000	15,000
Skin grafts	25% of burn benefit	25% of burn benefit
Emergency Dental Work (Crown)	250	350
Emergency Dental Work (Extraction)	60	90
Eye Injury (removal of foreign object)	60	100
Eye Injury (surgery)	225	350
Torn Knee Cartilage (surgery with no repair or if cartilage is shaved)	150	225
Torn Knee Cartilage (surgical repair)	500	800
Laceration* (treated - no sutures)	20	30
Laceration* (sutures up to 2")	40	60
Laceration* (sutures 2" to 6")	160	240
Laceration* (sutures over 6")	320	480
Ruptured Disk (surgical repair)	500	800
Tendon, Ligament, Rotator Cuff (exploratory arthroscopic surgery with no repair)	275	425
Tendon, Ligament, Rotator Cuff (1, surgical repair)	550	825
Tendon, Ligament, Rotator Cuff (2 or more, surgical repair)	800	1,225
Concussion	150	225
Paralysis (paraplegia)	10,750	16,000
Paralysis (quadriplegia)	16,000	24,000

*Laceration benefits are a total of all lacerations per accident.

Common Injuries - DISLOCATIONS Closed / Open Reduction* (in $'s)

	Level 2	Level 4
Hip Joint	2,550 / 5,100	3,850 / 7,700
Knee	1,600 / 3,200	2,400 / 4,800
Ankle or foot bone(s) other than toes	1,000 / 2,000	1,500 / 3,000
Shoulder	1,000 / 2,000	1,600 / 3,200
Elbow	750 / 1,500	1,100 / 2,200
Wrist	750 / 1,500	1,100 / 2,200
Finger/Toe	175 / 350	275 / 550
Hand bone(s) other than fingers	750 / 1,500	1,100 / 2,200
Lower jaw	750 / 1,500	1,100 / 2,200
Collarbone	750 / 1,500	1,100 / 2,200
Partial dislocations	25% of the closed reduction amount	25% of the closed reduction amount

*Closed reduction of dislocation = non-surgical reduction of a completely separated joint; Open reduction of dislocation = surgical reduction of a completely separated joint.

Common Injuries - FRACTURES Closed / Open Reduction* (in $'s)

	Level 2	Level 4
Hip	2,000 / 4,000	3,000 / 6,000
Leg	1,500 / 3,000	2,500 / 5,000
Ankle	1,200 / 2,400	1,800 / 3,600
Kneecap	1,200 / 2,400	1,800 / 3,600
Foot (excluding toes, heel)	1,200 / 2,400	1,800 / 3,600
Upper arm	1,400 / 2,800	2,100 / 4,200
Forearm, hand, wrist (except fingers)	1,200 / 2,400	1,800 / 3,600
Finger, Toe	160 / 320	240 / 480
Vertebral body	2,240 / 4,480	3,360 / 6,720
Vertebral processes	960 / 1,920	1,440 / 2,880
Pelvis (except coccyx)	2,250 / 4,500	3,200 / 6,400
Coccyx	200 / 400	400 / 800
Bones of the face (except nose)	800 / 1,600	1,200 / 2,400
Nose	400 / 800	600 / 1,200

Common Injuries - FRACTURES Closed / Open Reduction* (cont)

	Level 2	Level 4
Upper jaw	1,000 / 2,000	1,500 / 3,000
Lower jaw	960 / 1,920	1,440 / 2,880
Collarbone	960 / 1,920	1,440 / 2,880
Rib or ribs	300 / 600	400 / 800
Skull - Simple (except bones of the face)	1,000 / 2,000	1,400 / 2,800
Skull - Depressed (except bones of the face)	2,000 / 4,000	3,000 / 6,000
Sternum	240 / 480	360 / 720
Shoulder blade	1,200 / 2,400	1,800 / 3,600
Chip fractures	25% of the closed reduction amount	25% of the closed reduction amount

*Closed reduction of fracture = non-surgical; Open reduction of fracture = surgical.

A Proposal for County of Fresno

Compass Accident Insurance plan description and rate information

Compass Accident Insurance can help your employees offset the costs associated with a covered accident. It provides fixed benefits for events tied to that accident. This is a limited benefit policy and does not satisfy the requirement of minimum essential coverage under the Affordable Care Act. The benefits can be used for any purpose the employee chooses, including things like health insurance deductibles, co payments, child-care, or home health care.

Offer C - Low Plan 24 hour

All Eligible Employees

Voluntary Level 2 - On/Off Job Coverage Monthly Cost* Employee Paid - Employee, Spouse, Children, Family			
Employee	**Employee & Spouse**	**Employee & Children**	**Family**
$4.73	$8.95	$9.15	$13.37

Level 2: Optional benefits and riders included (see Benefit Schedule for additional details):
Rehabilitation Facility Confinement benefit, Critical Care Unit Confinement benefit, Family Care benefit, Initial Doctor Visit benefit, Urgent Care Facility Treatment Benefit, Emergency Room Treatment benefit, Ground Ambulance benefit, Air Ambulance benefit, Follow up benefit, Chiropractic Treatment benefit, Phys or Occ Therapy benefit, Speech Therapy benefit, Major Diagnostic Exams benefit, Outpatient Surgery benefit, X-ray benefit, Sports Accident Benefit, Spouse Accident Rider, Children's Accident Rider, Accidental Death & Dismemberment (AD&D) Rider

* Cost includes Accident Insurance premium and the non-insurance service fee of $0.03 for Voya Travel Assistance.

Offer D - High Plan 24 hour

All Eligible Employees

Voluntary Level 4 - On/Off Job Coverage Monthly Cost* Employee Paid - Employee, Spouse, Children, Family			
Employee	**Employee & Spouse**	**Employee & Children**	**Family**
$7.16	$12.90	$14.49	$20.23

Level 4: Optional benefits and riders included (see Benefit Schedule for additional details):
Rehabilitation Facility Confinement benefit, Critical Care Unit Confinement benefit, Family Care benefit, Initial Doctor Visit benefit, Urgent Care Facility Treatment Benefit, Emergency Room Treatment benefit, Ground Ambulance benefit, Air Ambulance benefit, Follow up benefit, Chiropractic Treatment benefit, Phys or Occ Therapy benefit, Speech Therapy benefit, Major Diagnostic Exams benefit, Outpatient Surgery benefit, X-ray benefit, Sports Accident Benefit, Spouse Accident Rider, Children's Accident Rider, Accidental Death & Dismemberment (AD&D) Rider

* Cost includes Accident Insurance premium and the non-insurance service fee of $0.03 for Voya Travel Assistance.

A Proposal for County of Fresno

Compass Accident Additional Benefits (may vary by state)

Sports Accident Benefit

Offer C - Low Plan 24 hour	
All Eligible Employees	Pays an additional 25% of the Accident Hospital Care, Accident Care, or Common Injuries benefit amount listed above, up to a maximum benefit of $1,000, if the covered accident is the result of an organized sporting activity.
Offer D - High Plan 24 hour	
All Eligible Employees	Pays an additional 25% of the Accident Hospital Care, Accident Care, or Common Injuries benefit amount listed above, up to a maximum benefit of $1,000, if the covered accident is the result of an organized sporting activity.

Compass Accident Insurance Riders - Benefit schedules (may vary by state)

Spouse Accident Rider

Offer C - Low Plan 24 hour	
All Eligible Employees	Matches the employee schedule.
Offer D - High Plan 24 hour	
All Eligible Employees	Matches the employee schedule.

Children's Accident Rider

Offer C - Low Plan 24 hour	
All Eligible Employees	Matches the employee schedule.
Offer D - High Plan 24 hour	
All Eligible Employees	Matches the employee schedule.

Accidental Death and Dismemberment (AD&D) Rider

Offer C - Low Plan 24 hour: All Eligible Employees	
Benefit Level	Voluntary: Level 2

A Proposal for County of Fresno

Compass Accident Insurance Riders — Benefit schedules (may vary by state)

Accidental Death and Dismemberment (AD&D) Rider

Offer D - High Plan 24 hour: All Eligible Employees	
Benefit Level	Voluntary: Level 4

Accidental Death (in $'s)

	Level 2	Level 4
Common Carrier		
Employee	65,000	100,000
Spouse	30,000	50,000
Children	15,000	25,000
Other Accidental Death		
Employee	30,000	50,000
Spouse	12,500	20,000
Children	6,000	10,000

Accidental Dismemberment (in $'s)

	Level 2	Level 4
Loss of both hands or both feet or sight in both eyes	20,000	28,000
Loss of one hand or one foot AND sight in one eye	14,000	22,000
Loss of one hand AND one foot	14,000	22,000
Loss of one hand OR one foot	7,500	12,500
Loss of two or more fingers or toes	1,200	1,800
Loss of one finger or toe	750	1,250

Rider Form numbers (may vary by state):
Spouse Accident Rider Form #: RL-ACC3-SPR-16
Children's Accident Rider Form #: RL-ACC3-CHR-16
Accidental Death & Dismemberment (AD&D) Rider Form #: RL-ACC3-ADR-16

Definitions

Compass Accident Insurance terms (may vary by state)

The following section provides a brief overview of Accident Insurance riders. Benefit provisions may vary by state and benefits may not be available in all states. Please ask your Voya Employee Benefits Sales Representative for more information.

Compass Accident Riders	
Spouse Accident Rider	The Spouse Accident Rider provides accident insurance for an eligible spouse. The employee must have coverage in order to include the Spouse Accident Rider.
Children's Accident Rider	The Children's Accident Rider provides coverage for an employee's eligible children from birth to termination age. One rider covers all eligible children. The employee must have coverage in order to include the Children's Accident Rider.
Accidental Death and Dismemberment (AD&D) Rider	The AD&D Rider covers all who are insured under the certificate and spouse and children's riders. See the schedule to view the plan options and benefit levels provided.

Issued by ReliaStar Life Insurance Company
A member of the Voya® family of companies

Compass Critical Illness Insurance

A Proposal for County of Fresno

Compass Critical Illness Insurance — Plan summary, and benefit and rider schedules

Offer B - BAFO:

	All Eligible Employees
Plan design	**Per Diagnosis Plan** Insured persons can receive a lump–sum benefit payment (100% of the benefit associated with that condition) for covered conditions under each module selected by the employer. This offer includes a **2 times** total benefit amount multiplier, meaning covered conditions which may naturally recur are payable up to the proposed multiple. Once the benefit multiplier has been claimed for a covered condition, the insured is no longer able to receive benefit payments for the same covered condition.
Covered benefit modules, additional benefits & riders	**Base Module** Heart attack (cardiac arrest is not a heart attack) – 100% Cancer (Invasive) – 100% Stroke – 100% Major organ transplant* – 100% Coronary artery bypass - 25% Cancer (Non-invasive) - 25% * Major organ transplant means the irreversible failure of your heart, lung, pancreas, entire kidney or liver, or any combination thereof, determined by a Physician specialized in care of the involved organ. **Major Organ Module** Severe burns – 100% Transient ischemic attacks (TIA) – 10% Ruptured or dissecting aneurysm – 10% Abdominal aortic aneurysm – 10% Thoracic aortic aneurysm – 10% Open heart surgery for valve replacement or repair – 25% Transcatheter heart valve replacement or repair – 10% Coronary angioplasty – 10% Implantable (or Internal) cardioverter defibrillator (ICD) placement – 25% Pacemaker placement – 10% **Quality of Life Module** Loss of sight, hearing or speech – 100% Coma – 100% Multiple sclerosis – 50% Amyotrophic lateral sclerosis (ALS) – 50% **Riders** Spouse Critical Illness Rider Children's Critical Illness Rider Additional Child Diseases Module Wellness Benefit Rider

Issued by ReliaStar Life Insurance Company
A member of the Voya® family of companies

A Proposal for County of Fresno

Compass Critical Illness Insurance — Plan summary, and benefit and rider schedules

Offer B - BAFO: (continued)

	All Eligible Employees (continued)
Covered benefit amount	**Employee** Benefit amount: Choice of $10,000 or $20,000 **Spouse** Spouse coverage matches employee benefit schedule, additional benefits and riders. Benefit amount: Choice of $5,000 or $10,000 **Child** Children's coverage matches employee benefit schedule, additional benefits and riders. Benefit amount: Choice of $5,000 or $10,000 Additional Child Diseases are payable at 100% of the benefit amount elected and include: Cerebral Palsy; Congenital Birth Defects; Cystic Fibrosis; Down Syndrome; Gaucher Disease, Type II or III; Infantile Tay Sachs; Niemann-Pick Disease; Pompe Disease; Type IV Glycogen Storage Disease
Benefit reduction schedule	None
Diagnosis separation periods	Time period between diagnoses: 12 months for subsequent (same) diagnoses; 0 months for different diagnoses
Pre-existing condition exclusion	New Coverage Supplemental: None

Rider Form numbers (may vary by state):

Spouse Critical Illness Rider Form #: RL-CI4-SPR-16
Children's Critical Illness Rider Form #: RL-CI4-CHR-16

A Proposal for County of Fresno

Compass Critical Illness Insurance - Rider schedules

Wellness Benefit Rider

Offer B - BAFO: All Eligible Employees

	Voluntary:
Employee	$50
Spouse	$50
Child	50% of employee's Wellness Benefit amount, to a maximum of $100 for all children

Rider Form numbers (may vary by state):
Wellness Benefit Rider Form #: RL-CI4-WELL-16

A Proposal for County of Fresno

Compass Critical Illness Insurance plan description and rate information

Compass Critical Illness Insurance provides a lump-sum benefit following the diagnosis of a covered illness or condition. This is a limited benefit policy and does not satisfy the requirement of minimum essential coverage under the Affordable Care Act. Employees can use the benefit as they see fit to help navigate back to health and to work.

Offer B - BAFO

All Eligible Employees

Voluntary Critical Illness employee coverage Employee-paid - Employee monthly rate per $1,000* Attained age	
	Uni-Tobacco
Under 30	$0.26
30-39	$0.35
40-49	$0.78
50-59	$1.92
60-64	$3.17
65-69	$4.27
70+	$6.58

* The cost of the Wellness Benefit Rider is not included in the Critical Illness rate.

All Eligible Employees: Optional benefits and riders included (see Benefit Schedule for additional details): N/A

Offer B - BAFO

Wellness Benefit Rider Employee-paid - Employee Monthly rate	
	Employee
All Eligible Employees	$1.18

A Proposal for County of Fresno

Compass Critical Illness Insurance plan description and rate information

Offer B - BAFO

All Eligible Employees

Voluntary Spouse Critical Illness Rider Employee-paid - Spouse monthly rate per $1,000* Attained age	
	Uni-Tobacco
Under 30	$0.30
30-39	$0.39
40-49	$0.85
50-59	$2.22
60-64	$3.82
65-69	$5.14
70+	$6.90

* The cost of the Wellness Benefit Rider is not included in the Critical Illness rate.

All Eligible Employees: Optional benefits and riders included (see Benefit Schedule for additional details):
N/A

Offer B - BAFO

Voluntary Children's Critical Illness Rider Composite monthly rate	
	Children
All Eligible Employees	$1.40 for $5,000 $2.80 for $10,000

Employee-paid - Children
Optional benefits and riders included (see Benefit Schedule for additional details): Additional Child Diseases Module

Offer B - BAFO

Wellness Benefit Rider Employee-paid - Spouse & children Monthly rate		
	Spouse	Children
All Eligible Employees	$1.18	The Wellness Benefit Rider is included in the Children's Critical Illness coverage rate above.

Definitions

Compass Critical Illness Insurance terms (may vary by state)

The following section provides a brief overview of Critical Illness Insurance plan design options, covered benefit modules, additional benefits and related riders. Benefit provisions may vary by state and riders may not be available in all states. Please ask your Voya Employee Benefits Sales Representative for more information.

Plan design	
Diagnosis separation period	This plan pays based on a definition for different diagnosis. A diagnosis of a Critical Illness that is for a different illness/condition than a previously diagnosed illness/condition (0 months separation period). It includes a subsequent diagnosis of a Critical Illness that is for the same illness/condition as a Critical Illness for which benefits were payable under the Policy, or the subsequent diagnosis of a Critical Illness that is for the same illness/condition as an illness/condition diagnosed prior to the insured's coverage effective date under the Policy, if the subsequent diagnosis occurs more than 12 months after the date of the previous diagnosis.
Total maximum benefit amount	This offer includes a **2 times** total benefit amount multiplier, which means each covered condition which can naturally recur are payable up to the multiple proposed. This is the maximum amount payable under the Critical Illness policy. Any payment for a spouse and/or children does not reduce the employee's total maximum benefit amount or vice versa. However, if the employee's coverage terminates due to receipt of the total maximum benefit amount payable, then spouse and children coverage also terminates.

Covered modules & additional benefits	
Base Module	This module pays a benefit for any diagnosis related to the core benefits in the market and is the "base" element of Critical Illness Insurance.
Major Organ Module	This module pays a benefit for diagnoses related to major organs and systems. Conditions and the payout percentages included in this module are defined in the benefits schedule above.
Quality of Life Module	This module focuses on diagnoses that directly impact the individual's quality of life, and which may result in home modifications and/or additional care. Conditions and the payout percentages included in this module are defined in the benefits schedule above.

Covered riders	
Spouse Critical Illness Rider	This rider provides Critical Illness Insurance for an eligible spouse. The employee must have coverage in order to include the Spouse Critical Illness Rider.
Children's Critical Illness Rider	This rider provides coverage for an employee's eligible children from birth to termination age. One rider covers all eligible children. The employee must have coverage in order to include the Children's Critical Illness Rider.
Additional Child Diseases Module	This module focuses on conditions that generally develop in utero or childhood. This module is only available with the Children's Critical Illness Rider and provides protection in addition to any other modules elected by the employer. Conditions and the payout percentages included in this module are defined in the benefits schedule above.
Wellness Benefit Rider	The rider pays a benefit when a covered person has a health screening test.

Compass Hospital Confinement Indemnity Insurance

A Proposal for County of Fresno

Compass Hospital Confinement Indemnity Insurance — Benefit Schedule (may vary by state)

	Offer B All Eligible Employees
Daily benefit amount	**Voluntary:** $100, $200
Hospital	**Voluntary:** $100, $200 (1 x Daily benefit amount) per day, up to 30 days per confinement
Critical care unit	**Voluntary:** $200, $400 (2 x Daily benefit amount) per day, up to 15 days per confinement
Rehabilitation facility	**Voluntary:** $50, $100 (0.5 x Daily benefit amount) per day, up to 30 days per confinement
Benefit waiting period*	0 Days
Benefit age reduction on daily benefit*	No Reductions
Pre-existing condition limitation*	**Voluntary:** None
Initial Confinement Benefit Rider	**Voluntary:** $500, $1000 (5 x Daily benefit amount)
Benefit age reduction	**Voluntary:** No Reductions
Wellness Benefit Rider	
Employee	**Voluntary:** $50
Spouse	**Voluntary:** $50
Child	**Voluntary:** 50% of employee's wellness benefit amount, to a maximum of $100 for all children
Wellness benefit waiting period*	0 Days

*Applies to all coverage types/levels.

Rider form numbers: (may vary by state):
Spouse Hospital Confinement Indemnity Rider Form #: RL-HI-SPR-12
Children's Hospital Confinement Indemnity Rider Form #: RL-HI-CHR-12
Wellness Benefit Rider Form #: RL-HI-WELL-12
Initial Confinement Benefit Rider Form #: RL-HI-ICN-12

A Proposal for County of Fresno

Compass Hospital Confinement Indemnity Insurance plan description and rate information

Compass Hospital Confinement Indemnity Insurance provides a benefit for eligible hospital confinements. This is a limited benefit policy and does not satisfy the requirement of minimum essential coverage under the Affordable Care Act. Employees can use the benefit as they choose – for instance, to help offset copays, coinsurance or deductibles that may be tied to a hospitalization or lost time from work.

Offer B

All Eligible Employees

Voluntary Composite Monthly rate Employee-paid – Employee, Spouse, Children, Family		
	$100 daily benefit*	$200 daily benefit*
Employee	$10.45	$23.40
Employee & Spouse	$20.70	$46.33
Employee & Children	$16.24	$35.82
Family	$26.49	$58.75

Voluntary: Optional Benefits and Riders included (see Benefit Schedule for additional details):
Spouse Hospital Confinement Indemnity Rider, Children's Hospital Confinement Indemnity Rider, Wellness Benefit Rider, Initial Confinement Benefit Rider

*Employee has choice of coverage level (Daily benefit amount) at enrollment.

Definitions

Compass Hospital Confinement Indemnity Insurance terms (may vary by state)

The following section provides a brief overview of Hospital Confinement Indemnity Insurance plan design options, covered conditions and related riders. Benefit provisions may vary by state and riders may not be available in all states. Please ask your Voya Employee Benefits Sales Representative for more information.

Compass Hospital Confinement Indemnity Riders	
Spouse Hospital Confinement Indemnity	The Spouse Hospital Confinement Indemnity Rider provides Hospital Confinement Indemnity insurance for an eligible spouse. The employee must have coverage in order to include the Spouse Hospital Confinement Indemnity Rider.
Children's Hospital Confinement Indemnity	The Children's Hospital Confinement Indemnity Rider provides coverage for an employee's eligible dependent children from birth to termination age (age may vary by state). One rider covers all eligible children.
Initial Confinement Benefit	This provides an additional payment of a multiple of the daily benefit amount after confinement in a covered facility as noted in the proposal. This benefit is limited to a maximum of four Initial Confinement Benefits per calendar year for all covered persons, but no more than one for each covered person.
Wellness Benefit	The Wellness Benefit Rider pays a benefit when a covered person has a health screening test.

EXHIBIT B

PROTECTED HEALTH INFORMATION CONFIDENTIALITY AGREEMENT

This Protected Health Information Confidentiality Agreement (the "Agreement") is entered into as of May 1, 2020 (the "Agreement Effective Date") by and between ReliaStar Life Insurance Company or its affiliate ReliaStar Life Insurance Company of New York (the "Company"), and the County of Fresno (the "Employer"). Employer shall be referred to herein as a "Disclosing Party".

RECITALS

A. The Employer is seeking to purchase or has purchased compass critical illness, accident, and hospital confinement indemnity policies (collectively, the "Policy") from the Company to cover employees.

B. The Disclosing Party may provide or disclose Protected Health Information (as defined below) to the Company in connection with the underwriting or payment of claims under the Policy.

C. The purpose of this agreement is to limit the use and disclosure of PHI by the Company to the purposes provided for herein and to provide reasonable assurances to Disclosing Party that the Company will maintain appropriate safeguards to protect PHI from any use or disclosure contrary to this Agreement and the Privacy Rule and Security Rule to the extent applicable (each as defined below).

SECTION 1: DEFINITIONS

(a) Breach. "Breach" shall have the same meaning given to such term in 45 C.F.R. § 164.402, as may be amended from time to time.

(b) Data Aggregation. "Data Aggregation" shall mean, with respect to Protected Health Information received by the Company, the combining of such Protected Health Information with Protected health information received by the Company under other stop-loss policy or policies, to permit data analyses as they relate to Health Care Operations.

(c) Designated Record Set. "Designated Record Set" shall have the same meaning as the term "designated record set" in 45 C.F.R § 164.501, as may be amended from time to time.

(d) Electronic Protected Health Information. "Electronic Protected Health Information" shall have the same meaning as "electronic protected health information" in 45 C.F.R. § 160.103, as may be amended from time to time.

(e) Health Care. "Health Care" shall have the same meaning as the term "health care" in 45 C.F.R. § 160.103, as may be amended from time to time.

(f) Health Care Operations. "Health Care Operations" shall have the same meaning as the term "health care operations" in 45 C.F.R. § 164.501, as may be amended from time to time and shall include, but not be limited to, underwriting of the Policy including activities of the Company for the reinsurance of the Policy.

(g) Individual. "Individual" shall have the same meaning as the term "individual" in 45 C.F.R § 160.103 and shall include a person's personal representative who is treated as the Individual in accordance with 45 C.F.R § 164.502(g), as each may be amended from time to time.

(h) Limited Data Set. "Limited Data Set" shall have the same meaning as the term "limited data set" in 45 C.F.R. § 164.514(e), as may be amended from time to time.

(i) Payment. "Payment" shall mean the same meaning as payment in 45 C.F.R. § 164.501, as may be amended from time to time, and shall include activities for the purpose of obtaining payment under the Policy and shall include, but not be limited to, Policy claim review, assessing primary and secondary coverage as between the Policy and the Group Health Plan under coordination of benefit provisions, pursuing subrogation claims and rights and submission of claim information under reinsurance policies or treaties between the Company and an insurance company that provides reinsurance benefits to the Company with respect to the Policy.

(j) Privacy Rule. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R part 160 and part 164, subparts A and E, as may be amended from time to time, as applied to the Company's use and disclosure of PHI provided for in this Agreement.

(k) Protected Health Information ("PHI"). "Protected Health Information" shall have the same meaning as the term "protected health information" in 45 C.F.R § 160.103, as may be amended from time to time, limited to the information received by the Company from any Disclosing Party.

(l) Required By Law. "Required By Law" shall have the same meaning as the term "required by law" in 45 C.F.R § 164.103, as many be amended from time to time.

(m) Secretary. "Secretary" shall mean the Secretary of the Department of Health and Human Services or his or her designee.

(n) Security Rule. "Security Rule" shall mean the Security Standards at 45 C.F.R. Parts 160 and Part 164, Subparts A and C, as may be amended from time to time, as applied to the Company's use and disclosure of PHI provided for in this Agreement.

(o) Transactions. "Transactions" shall have the same meaning as the term "transactions" in 45 C.F.R. § 164.103, as may be amended from time to time.

(p) Unsecured PHI. "Unsecured PHI" shall have the same meaning given to such term under 45 C.F.R. § 402), as may be amended from time to time.

SECTION 2: LIMITED DATA SET - PERMITTED USES AND DISCLOSURES

2.1 Permitted Uses and Disclosures. The Company may use PHI provided to it in the form of a Limited Data Set solely for the underwriting of the Policy. Except as provided for in Section 3 of this Agreement, the Company shall not use or disclose PHI under this Section for any other purpose.

2.2 Identification. The Company agrees not to undertake any action during the underwriting process and the placement of the Policy which may cause the PHI, including the Limited Data Set, to identify any Individual, nor shall the Company knowingly contact any Individual whose PHI is included in the Limited Data Set.

2.3 Policy Not Issued. Upon conclusion or termination of the underwriting process in which the Policy is not issued by the Company, the Company shall destroy any property received from any party which may be in the Company's possession including all PHI, confidential information, products, materials, memoranda, notes, records, reports, or other documents or photocopies of the same, including without limitation any of the foregoing recorded on any computer or any machine readable medium.

SECTION 3: PHI – PERMITTED USES AND DISCLOSURES

3.1 Purpose of PHI Disclosure. The Disclosing Party may provide and disclose PHI to the Company for underwriting of the Policy.

3.2 Permitted Uses. The Company may use PHI received from the Disclosing Party solely for the purpose for which it is provided as specified in Section 3.1 of this Agreement.

3.3 Permitted Disclosures. The Company may disclose PHI for underwriting and the payment of claims under the Policy provided that the Company obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and will be used or further disclosed only as Required by Law or for the purpose for which it was disclosed to the person (which purpose must be consistent with the limitations imposed upon the Company pursuant to this Agreement) and the person agrees to notify the Company of any use or disclosure of PHI of which it becomes aware in which the confidentiality of the information has been breached.

3.4 Required by Law. The Company may disclose the PHI if and to the extent that such disclosure is Required by Law.

3.5 Data Aggregation. The Company may use PHI to provide Data Aggregation services, including use of PHI for statistical compilations, reports, research and all other purposes allowed under applicable law.

3.6 De-identified Data. The Company may create de-identified PHI in accordance with the standards set forth in 45 C.F.R. § 164.514(b), as may be amended from time to time, and may use or disclose such de-identified data for any purpose.

SECTION 4: OBLIGATIONS OF THE COMPANY

4.1 Privacy of PHI. The Company will maintain appropriate safeguards to reasonably protect PHI from any intentional or unintentional use or disclosure contrary to this Agreement and the Privacy Rule.

4.2 Security of PHI. The Company shall ensure that its information security programs include appropriate administrative, physical and technical safeguards designed to prevent the use or disclosure of confidential information, such as the PHI received by the Company, contrary to this Agreement and the Security Rule.

4.3 Notification of Disclosures. The Company will report to the Disclosing Party any use or disclosure of PHI not provided for by this Agreement of which it becomes aware.

4.4 Notification of Breach. The Company will notify the Disclosing Party of any Breach of Unsecured PHI as soon as practicable, and no later than 30 days after discovery of such Breach. The Company's notification of a Breach will include: (a) the identification of each Individual whose Unsecured PHI has been, or is reasonably believed by the Company to have been, accessed, acquired or disclosed during the Breach; and (b) any particulars regarding the Breach that the Employer would need to include in its notification, as such particulars are identified in 45 C.F.R. § 164.404, as may be amended from time to time.

4.5 Mitigation. To the extent practicable, the Company will cooperate with the Disclosing Party's efforts to mitigate a harmful effect that is known to the Company of a use or disclosure of PHI not provided for in this Agreement.

4.6 HIPAA Compliance Support. The Company agrees to make internal practices, books, and records, including policies and procedures of its information security program, relating to the use and disclosure of confidential information, such as the PHI received by the Company, available to the Secretary, as requested by the Employer, or designated by the Secretary, for purposes of the Secretary determining the Employer's compliance with the Privacy Rule.

SECTION 5: OBLIGATIONS OF THE DISCLOSING PARTIES

5.1 Privacy Practices. The Employer will notify the Company of any changes to the limitation(s) in the Employer's notice of privacy practices in accordance with 45 C.F.R. § 164.520, as amended from time to time, to the extent that such a limitation may affect the Company's use or disclosure of PHI under this Agreement. The Employer will provide such notice no later than 15 days prior to the effective date of the limitation. The Employer confirms that the it's privacy notice discloses the use and disclosure of PHI for Health Care Operations and Payments as permitted by this Agreement.

5.2. Minimum Necessary. Disclosing Party shall limit PHI to the minimum necessary to accomplish the permitted uses and disclosures of the Company provided for in this Agreement when providing or disclosing PHI to the Company in accordance with 45 C.F.R. § 164.502(b) and 45 C.F.R. § 164.514(d), as each may be amended from time to time.

5.3. Payment and Health Care Operations Standards. Disclosing Party shall ensure that the use and disclosure of PHI by the Company complies with the standards of 45 C.F.R. § 164.506, as may be amended from time to time.

5.4 Electronic PHI. Disclosing Party shall not provide Electronic PHI to the Company in the form of "unsecured protected health information" as defined in 45 C.F.R. § 164.402, as may be amended from time to time.

6. TERM AND TERMINATION

6.1 Term. This Agreement will commence as of the Agreement Effective Date and will terminate in accordance with Section 2.3 or upon the termination of the Policy.

6.2 Termination for Cause. Upon either party's knowledge of a material breach by the other party of this Agreement, such party will provide written notice to the breaching party detailing the nature of the breach and providing an opportunity to cure the breach within 30 business days. Upon the expiration of such 30 day cure period, the non-breaching party may terminate this Agreement and, at its election, the Policy, if cure is not possible.

6.3 Effect of Termination. Upon termination of this Agreement or the Policy, the Company will: (a) extend the protections of this Agreement to all PHI retained by Company; (b) limit further uses and disclosures of such PHI to those purposes provided for in this Agreement for so long as the Company maintains such PHI; and (c) where possible, only disclose such PHI to a third party if the information has been de-identified in accordance with the standards set forth in 45 C.F.R. § 164.514(b), as may be amended from time to time. The parties acknowledge and agree that it is not feasible for the Company to return or destroy all PHI received by the Company under this Agreement; provided, however, that the Company's retention of PHI upon the termination of the Agreement or the Policy shall be solely for the purposes of complying with state record retention and insurance regulatory requirements applicable to the Policy and the Company as a licensed insurance company and for the Company's reinsurance obligations under reinsurance policies or treaties covering the Policy.

SECTION 7: SURVIVAL

The respective rights and obligations of the parties under Section 6.3 of this Agreement will survive the termination of this Agreement and the Policy.

SECTION 8: GENERAL

8.1 Relationship of the Parties under HIPAA. Disclosing Party agrees and acknowledges that the Company does not perform any function or service on behalf of any Group Health Plan and this Agreement should not be construed and does not establish any contractual relationship for services. The Company is not an agent or sub-contractor of any Disclosing Party or any Group Health Plan. Each Disclosing Party acknowledges and agrees that the Company does not provide Health Care to or for any Individual either directly or indirectly on behalf of any Group Health Plan. The Company does not conduct Transactions with any Group Health Plan or any Disclosing Party on behalf of any Group Health Plan and any Electronic PHI provided to the Company for the purposes of this Agreement shall not be subject to the administrative requirements of 45 C.F.R. § 162, as may be amended from time to time. Disclosing Party does not intend for the Company to maintain any PHI in a Designated Record Set.

8.2. Governing Law. This Agreement is governed by, and will be construed in accordance with, the laws of the State of California.

8.3 Successors and Assigns. This Agreement and each party's obligations hereunder will be binding on the representatives, assigns, and successors of such party and will inure to the benefit of the assigns and successors of such party. No party may assign this Agreement without the prior written consent of Company, which will not be unreasonably withheld.

8.4 Severability. If any part of a provision of this Agreement is found illegal or unenforceable, it will be enforced to the maximum extent permissible, and the legality and enforceability of the remainder of that provision and all other provisions of this Agreement will not be affected.

8.5 Notices. All notices relating to the parties' legal rights and remedies under this Agreement will be provided in writing to a party, will be sent to its address set forth in the Policy, or to such other address as may be designated by that party by notice to the sending party, and will reference this Agreement.

8.6 Amendment and Waiver. This Agreement may be modified, or any rights under it waived, only by a written document executed by the authorized representatives of the parties. Nothing in this Agreement will confer any right, remedy, or obligation upon anyone other than the Disclosing Parties and the Company.

8.7 Entire Agreement. This Agreement is the complete and exclusive agreement between the parties with respect to the subject matter hereof, superseding and replacing all prior agreements, communications, and understandings (written and oral) regarding its subject matter.

8.8 Headings and Captions. The headings and captions of the various subdivisions of this Agreement are for convenience of reference only and will in no way modify, or affect the meaning or construction of any of the terms or provisions hereof.

8.9 Counterparts. This Agreement may be signed in counterparts, which together will constitute one agreement.

IN WITNESS WHEREOF, the parties have caused this Agreement to be signed by their duly authorized representatives or officers, effective as of the Agreement Effective Date.

ReliaStar Life Insurance Company and its affiliate ReliaStar Life Insurance Company of New York	**County of Fresno**
Address: **20 Washington Avenue South** **Minneapolis, Minnesota 55401**	**Address:** **2220 Tulare Street, 14th Floor** **Fresno, CA 93721**
Signed:	**Signed:**
NAME Title	**Ernest Buddy Mendes** Chairman of the Board of Supervisors of the County of Fresno
Date:	**Date:**

EXHIBIT C

Voya Data Security Addendum

1. Definitions.

"Affected Persons" means Client's and its Affiliate's former and current employees whose Personal Information ("PI") may have been disclosed or compromised as a result of an Information Security Incident.

"**Affiliates**" means any entities that, now or in the future, control, are controlled by, or are under common control with Client. An entity will be deemed to control another entity if it has the power to direct or cause the direction of the management or policies of such entity, whether through ownership, voting securities, contract, or otherwise.

"Confidential Information" means (a) non-public information concerning the Disclosing Party; its affiliates; and their respective businesses, products, processes, and services, including technical, marketing, agent, customer, financial, personnel, and planning information; (b) PI; (c) trade secrets; and (d) any other information that is marked confidential or which, under the circumstances surrounding disclosure, the Non-Disclosing Party should know is treated as confidential by the Disclosing Party. Except with respect to PI, which will be treated as Confidential Information under all circumstances, Confidential Information will not include (A) information lawfully obtained or developed by the Non-Disclosing Party independently of the Disclosing Party's Confidential Information and without breach of any obligation of confidentiality; or (B) information that enters the public domain without breach of any obligation of confidentiality. All Confidential Information will remain the property of the Disclosing Party.

"Information Security Incident" means any breach of security or cyber security incident impacting Voya that has a reasonable likelihood of (a) resulting in the loss or unauthorized access, use or disclosure of Client PI; (b) materially affecting the normal operation of Voya; or (c) preventing Voya from complying with all of the privacy and security requirements set forth in this Agreement.

"Law" means all U.S. and non-U.S. laws, ordinances, rules, regulations, declarations, decrees, directives, legislative enactments and governmental authority orders and subpoenas.

"PI" means any information or data that (a) identifies an individual, including by name, signature, address, telephone number or other unique identifier; (b) can be used to identify or authenticate an individual, including passwords, PINs, biometric data, unique identification numbers (*e.g.*, social security numbers), answers to security questions or other personal identifiers; (c) is "non-public personal information" as defined in the Gramm-Leach-Bliley Act 15 U.S.C. § 6809(4) or "protected health information" as defined in 45 C.F.R. § 160.103; or (d) is an account number or credit card number or debit card number, in combination with any required security code, access code, or password, that would permit access to an individual's financial account.

"**Services**" means the services that Voya provides to Client pursuant to this Agreement.

"Voya Personnel" means Voya's employees and subcontractors engaged in the performance of Services.

2. Data Security.

2.1. Security Standards and Controls.

(a) Voya will establish and maintain:
- (i) administrative, technical, and physical safeguards against the destruction, loss, or alteration of Confidential Information; and
- (ii) appropriate security measures to protect Confidential Information, which measures meet or exceed the requirements of all applicable Laws relating to personal information security.

(b) In addition, Voya will implement and maintain the following information security controls:
- (i) privileged access rights will be restricted and controlled;
- (ii) an inventory of assets relevant to the lifecycle of information will be maintained;
- (iii) network security controls will include, at a minimum, firewall and IDS services;
- (iv) detection, prevention and recovery controls to protect against malware will be implemented;
- (v) information about technical vulnerabilities of Voya's information systems will be obtained and evaluated in a timely fashion and appropriate measures taken to address the risk;

(vi) detailed event logs recording user activities, exceptions, faults, access attempts, operating system logs, and information security events will be produced, retained and regularly reviewed; and

(vii) development, testing and operational environments will be separated to reduce the risks of unauthorized access or changes to the operational environment.

2.2. Information Security Policies. Voya will implement and maintain written policies and procedures that address the following areas:

(a) information security;
(b) data governance and classification;
(c) access controls and identity management;
(d) asset management;
(e) business continuity and disaster recovery planning and resources;
(f) capacity and performance planning;
(g) systems operations and availability concerns;
(h) systems and network security;
(i) systems and application development, quality assurance and change management;
(j) physical security and environmental controls;
(k) customer data privacy;
(l) patch management;
(m) maintenance, monitoring and analysis of security audit logs;
(n) vendor and third party service provider management; and
(o) incident response, including clearly defined roles and decision making authority and a logging and monitoring framework to allow the isolation of an incident.

2.3. Subcontractors. Voya will implement and maintain policies and procedures to ensure the security of Confidential Information and related systems that are accessible to, or held by, third party service providers. Voya will 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:

(a) the use of encryption to protect sensitive PI in transit, and the use of encryption or other mitigating controls to protect sensitive PI at rest;
(b) prompt notice to be provided in the event of a cyber security incident;
(c) the ability of Voya or its agents to perform information security assessments; and
(d) representations and warranties concerning adequate information security.

2.4. Encryption Standards, Multifactor Authentication and Protection of Confidential Information.

(a) Voya will implement and maintain cryptographic controls for the protection of Confidential Information, including the following:

(i) use of an encryption standard equal to or better than the industry standards described in National Institute for Standards and Technology Special Publication 800-175B (or such higher encryption standard required by applicable Law) to protect Confidential Information in transit over un-trusted networks;
(ii) use of cryptographic techniques to provide evidence of the occurrence or nonoccurrence of an event or action;
(iii) use of cryptographic techniques to authenticate users and other system entities requesting access to or transacting with system users, entities and resources; and
(iv) development and implementation of policies on the use, protection and lifetime of cryptographic keys through their entire lifecycle.

(b) In addition to the controls described in clause (a) above, Voya will:

(i) implement multi-factor authentication for all remote access to Voya's networks;
(ii) ensure that no Client PI is (A) placed on unencrypted mobile media, CDs, DVDs, equipment, or laptops or (B) stored or transmitted outside the United States; and
(iii) ensure that media containing Confidential Information is protected against unauthorized access, misuse or corruption during transport.

2.5. Information Security Roles and Responsibilities. Voya will employ personnel adequate to manage Voya's information security risks and perform the core cyber security functions of identify, protect, detect, respond and recover. Voya will designate a qualified employee to serve as its Chief Information Security Officer ("**CISO**") responsible for overseeing and implementing its information security program and enforcing its information security policies. Voya will define roles and responsibilities with respect to information security, including by identifying responsibilities for the protection of individual assets, for carrying out specific information security processes, and for information security risk management activities, including acceptance of residual risks. These responsibilities should be supplemented, where appropriate, with more detailed guidance for specific sites and information processing facilities.

2.6. Segregation of Duties. Voya must segregate duties and areas of responsibility in order to reduce opportunities for unauthorized modification or misuse of Voya's assets and ensure that no single person can access, modify or use assets without authorization or detection. Controls should be designed to separate the initiation of an event from its authorization. If segregation is not reasonably possible, other controls such as monitoring of activities, audit trails and management supervision should be utilized. Development, testing, and operational environments should be separated to reduce the risks of unauthorized access or changes to the operational environment.

2.7. Information Security Awareness, Education and Training. Voya will provide regular information security education and training to all Voya Personnel, as relevant for their job function. In addition, Voya will provide mandatory training to information security personnel and require key information security personnel to stay abreast of changing cyber security threats and countermeasures.

2.8. Vulnerability Assessments. Voya will conduct monthly vulnerability assessments that meet the following criteria:

(a) all production servers and network devices must be scanned at least monthly;
(b) all findings must be risk rated;
(c) all findings must be tracked to closure based on risk; and
(d) tools used for scanning must have signatures updated at least monthly with the latest vulnerability. Voya will implement and maintain a formal process for tracking and resolving issues in a timely fashion.

2.9. Physical and Environmental Security. Voya will ensure that all sites are physically secure, including the following:

(a) sound perimeters with no gaps where a break-in could easily occur;
(b) exterior roof, walls and flooring of solid construction and all external doors suitable protected against unauthorized access with control mechanisms such as locks, bars, alarms, etc.;
(c) all doors and windows to operational areas locked when unattended;
(d) equipment protected from power failures and other disruptions caused by failures in supporting utilities;
(e) closed-circuit television cameras at site entry/ exit points; badge readings/ turn styles at all site entry points, or other means to prevent unauthorized access; and
(f) visitor sign-in/ mandatory escort at site.

2.10. Information Security Incident Notification.

(a) In the event of any Information Security Incident, Voya will, at its sole expense: promptly (and in any event within 72 hours after Voya confirms an Information Security Incident) report such Information Security Incident to Client by sending an email to the email address designed by Client, summarizing in reasonable detail the effect on Client, if known, and designating a single point of contact at Voya who will be
  (i) available to Client for information and assistance related to the Information Security Incident;
  (ii) investigate such Information Security Incident, perform a root cause analysis, develop a corrective action plan and take all necessary corrective actions;
  (iii) mitigate, as expeditiously as possible, any harmful effect of such Information Security Incident and cooperate with Client in any reasonable and lawful efforts to prevent, mitigate, rectify and remediate the effects of the Information Security Incident;
  (iv) provide a written report to Client containing all information necessary for Client to determine compliance with all applicable laws, including the extent to which notification to affected persons or to government or regulatory authorities is required; and

(v) cooperate with Client in providing any filings, communications, notices, press releases or reports related to such Information Security Incident.

(b) In addition to the other indemnification obligations of Voya set forth in this Agreement, Voya will indemnify, defend and hold harmless Client from and against any and all claims, suits, causes of action, liability, loss, costs and damages, including reasonable attorneys' fees, arising out of or relating to any Information Security Incident, which may include, without limitation:

(i) expenses incurred to provide notice to Affected Persons and to law-enforcement agencies, regulatory bodies or other third parties as required to comply with law;

(ii) expenses related to any reasonably anticipated and commercially recognized consumer data breach mitigation efforts, including, but not limited to, costs associated with the offering of credit monitoring or a similar identify theft protection or mitigation product for a period of at least twelve (12) months or such longer time as is required by applicable laws or any other similar protective measures designed to mitigate any damages to the Affected Persons; and

(iii) fines or penalties that Client pays to any governmental or regulatory authority under legal or regulatory order as a result of the Information Security Incident.

2.11. Risk Assessments. Upon Client's request no more than once per year, Voya will complete an industry standard information security questionnaire and provide relevant Service Organization Control ("**SOC**") audit reports, when available. Voya's standard security requirements are set forth in Exhibit A. Voya represents and warrants that, as of the Effective Date, the statements in Exhibit A are true and correct in all material respects.

2.12. Penetration Testing. If any Services to be provided by Voya include the hosting or support of one or more externally facing applications that can be used to access systems that store or process Client data, the terms of this Section will apply.

(a) At least once every 12 months during the Term and prior to any major changes being moved into production, Voya will conduct a Valid Penetration Test (as defined below) on each internet facing application described above. As used herein, a "**Valid Penetration Test**" means a series of tests performed by a team of certified professionals, which tests mimic real-world attack scenarios on the information system under test and include, without limitation, the following:

(i) information-gathering steps and scanning for vulnerabilities;

(ii) manual testing of the system for logical flaws, configuration flaws, or programming flaws that impact the system's ability to ensure the confidentiality, integrity, or availability of Client's information assets;

(iii) system-compromise steps;

(iv) escalation-of-privilege steps; and

(v) assignment of a risk rating for each finding based on the level of potential risk exposure to Client's brand or information assets.

(b) Upon Client's request, Voya will review the results of the most recent Valid Penetration Test with Client and provide the following documentation for Client's review:

(i) the penetration test management summary (which may be redacted to ensure confidentiality of the technical details of the flaws in the system under test) showing the testing methodology used for performing the testing, which report will include information-gathering steps, vulnerability scanning, manual testing, system compromise, and escalation of privilege steps.

3. Privacy and PII.

3.1. With respect to any PI, Voya will:

(a) process all PI accessed by Voya only to perform its obligations under this Agreement;

(b) not use such PI for any other purpose, including for its own commercial benefit;

(c) treat all PI as Confidential Information;

(d) comply with the provisions of this Agreement to return, store or destroy the PI; and

(e) comply with all applicable Laws with respect to processing of PI.

3.2. As needed to comply with applicable Laws concerning the processing of PI or personal information security, or to the extent required by any changes in such Laws or the enactment of new Laws, the Parties agree to work cooperatively and in good faith to amend this Agreement in a mutually agreeable and timely manner, or to enter into further mutually agreeable agreements in an effort to comply with any such Laws applicable to the Parties. If the Parties cannot so agree, or if Voya cannot comply with the new or additional requirements, Client may terminate this Agreement upon written notice to Voya.

4. Confidential Information.

4.1. Confidential Information. Either Party ("**Disclosing Party**") may disclose Confidential Information to the other Party ("**Non-Disclosing Party**") in connection with this Agreement.

4.2. Use and Disclosure of Confidential Information. The Non-Disclosing Party agrees that it will disclose the Disclosing Party's Confidential Information only to its employees, agents, consultants, and contractors who have a need to know and are bound by obligations of confidentiality no less restrictive than those contained in this Agreement. In addition, Voya agrees that it will use the Disclosing Party's Confidential Information only for the purposes of performing its obligations under this Agreement. The Non-Disclosing Party will use all reasonable care in handling and securing the Disclosing Party's Confidential Information and will employ all security measures used for its own proprietary information of similar nature. These confidentiality obligations will not restrict any disclosure of Confidential Information required by Law or by order of a court, regulatory authority or governmental agency; provided, that the Non-Disclosing Party will limit any such disclosure to the information actually required to be disclosed. Notwithstanding anything to the contrary, Client may fully comply with requests for information from regulators of Client and the Client Affiliates.

4.3. Treatment of Confidential Information Following Termination. Promptly following the termination or expiration of this Agreement, or earlier if requested by the Disclosing Party, the Non-Disclosing Party will return to the Disclosing Party any and all physical and electronic materials in the Non-Disclosing Party's possession or control containing the Disclosing Party's Confidential Information. The materials must be delivered via a secure method and upon such media as may be reasonably required by the Disclosing Party. Alternatively, with the Disclosing Party's prior written consent, the Non-Disclosing Party may permanently destroy or delete the Disclosing Party's Confidential Information and, if requested, will promptly certify the destruction or deletion in writing to the Disclosing Party. Notwithstanding the foregoing, if the Non-Disclosing Party, due to requirements of applicable Law, must retain any of the Disclosing Party's Confidential Information, or is unable to permanently destroy or delete the Disclosing Party's Confidential Information as permitted above within 60 days after termination of this Agreement, the Non-Disclosing Party will so notify the Disclosing Party in writing, and the Parties will confirm any extended period needed for permanent destruction or deletion of the Disclosing Party's Confidential Information. All Confidential Information in the Non-Disclosing Party's possession or control will continue to be subject to the confidentiality provisions of this Agreement. The methods used to destroy and delete the Confidential Information must ensure that no Confidential Information remains readable and cannot be reconstructed so to be readable. Destruction and deletion must also comply with the following specific requirements:

MEDIUM	DESTRUCTION METHOD
Hard copy	Shredding, pulverizing, burning, or other permanent destruction method
Electronic tangible media, such as disks and tapes	Destruction or erasure of the media
Hard drive or similar storage device	Storage frame metadata removal to hide the organizational structure that combines disks into usable volumes and physical destruction of the media with a Certificate of Destruction (COD)

4.4. Period of Confidentiality. The restrictions on use, disclosure, and reproduction of Confidential Information set forth in this Section will, with respect to PI and Confidential Information that constitutes a "trade secret" (as that term is defined under applicable Law), be perpetual, and will, with respect to other Confidential Information, remain in full force and effect during the term of this Agreement and for three years following the termination or expiration of this Agreement.

4.5. Injunctive Relief. The Parties agree that the breach, or threatened breach, of any of the confidentiality provisions of this Agreement may cause irreparable harm without adequate remedy at law. Upon any such breach or threatened breach, the Disclosing Party will be entitled to injunctive relief to prevent the Non-Disclosing Party from commencing or continuing any action constituting such breach, without having to post a bond or other security and without having to prove the inadequacy of other available remedies. Nothing in this Section will limit any other remedy available to either Party.

5. Cyber Liability Insurance. During the Term, Voya will, at its own cost and expense, obtain and maintain in full force and effect, with financially sound and reputable insurers, cyber liability insurance to cover Voya's obligations under this Addendum. Upon execution of the Agreement, Voya will provide Client with a certificate of insurance evidencing the following coverage and amount with such insurer:

Risk Covered: Network Security (a.k.a. Cyber/IT)
Limits: >$55,000,000
Policy dates: May 2, 2018 – May 2, 2019

6. Disaster Recovery and Business Continuity Plan. Voya maintains, and will continue to maintain throughout the Term, (a) a written disaster recovery plan ("**Disaster Recovery Plan**"), which Disaster Recovery Plan is designed to maintain Client's access to services and prevent the unintended loss or destruction of Client data; and (b) a written business continuity plan ("**BCP**") that permits Voya to recover from a disaster and continue providing services to customers, including Client, within the recovery time objectives set forth in the BCP. Upon Client's reasonable request, Voya will provide Client with evidence of disaster recovery test date and result outcome.

Exhibit A
Security Requirements

FC:	Foundation Controls
FC-1:	Information Asset Management
FC-1.1	Voya implements and maintains an inventory list and assigns ownership for all computing assets including, but not limited to, hardware and software used in the accessing, storage, processing, or transmission of Client PI.
FC-1.2	Voya reviews and updates the inventory list of assets for correctness and completeness at least once every 12 months and updates the inventory list as changes are made to the computing assets.
FC-2:	Data Privacy and Confidentiality
FC-2.1	Voya will maintain an Information and Risk Management policy that is reviewed and approved by management at least every 2 years.
FC-2.2	Voya protects the privacy and confidentiality of all Client PI received, disclosed, created, or otherwise in Voya's possession by complying with the following requirements:
FC-2.2A	Such information is encrypted at rest on mobile devices (including mobile storage devices), portable computers, and in transit over un-trusted networks with an encryption standard equal to or better than AES 256 bit encryption or such higher encryption standard required by applicable Law.
FC-2.2B	All hardcopy documents and removable media are physically protected from unauthorized disclosure by locking them in a lockable cabinet or safe when not in use and ensuring that appropriate shipping methods (tamper-proof packaging sent by special courier with signatures) are employed whenever the need to physically transport such documents and removable media arises.
FC-2.2C	All media is labeled and securely stored in accordance with Voya policies.
FC-2.2D	All electronic media is securely sanitized or destroyed when no longer required in accordance with industry standards.
FC-3:	Configuration Management
FC-3.1	Voya implements and maintains accurate and complete configuration details (e.g., Infrastructure Build Standards) for all computing assets used in accessing, storing, processing, or transmitting Client PI.
FC-3.2	Voya reviews configuration details of the computing assets at least once every 12 months to validate that no unauthorized changes have been made to the assets.
FC-3.3	Voya updates the configuration details of all computing assets used to access, process, store, or transmit Client PI as configuration changes take place.
FC-4:	Operating Procedures and Responsibilities
FC-4.1	Voya implements and maintains operational procedures for information processing facilities and designates specific roles or personnel responsible for managing and maintaining the quality and security of such facilities, including, but not limited to, formal handover of activity, status updates, operational problems, escalation procedures and reports on current responsibilities. Voya IT policies and standards document the policies and procedures for job scheduling processes and tools.
FC-4.2	Voya updates the operational procedures as changes take place and performs a comprehensive review and update of the procedures at least once every 2 years.
FC-5:	Security Awareness and Training
FC-5.1	Voya performs pre-employment background checks, including criminal history for 7 years, drug screening, credit score and history (if applicable), credentials verification (if applicable), and educational background.
FC-5.2	Voya implements and maintains a documented security awareness program for all Voya Personnel which covers access to Client PI.

FC-5.3	Voya's security awareness program includes security requirements, acceptable use of computing assets, legal responsibilities, and business controls, as well as training in the correct use of information processing facilities and physical security controls.
FC-5.4	Voya ensures that all Voya Personnel complete security awareness training prior to being provided access to Client PI and at least annually thereafter. Voya provides mandatory annual training programs that include security awareness training to all Personnel.
UA:	User Access Controls
UA-1:	User Access Controls
UA-1.1	Voya implements and maintains identity management system(s) and authentication process(es) for all systems that access, process, store, or transmit Client PI.
UA-1.2	Voya ensures that the following user access controls are in place:
UA-1.2A	The "Least Privilege" concept is implemented ensuring no user has more privileges than they require in performing their assigned duties.
UA-1.2B	Users requiring elevated privileges as a normal part of their job responsibilities have a regular, non-privileged account to perform regular business functions.
UA-1.2C	All users have an individual account which cannot be shared.
UA-1.2D	Account Names/IDs are constructed not to reveal the privilege level of the account or position of the account holder.
UA-1.2E	System- or application-level service accounts are owned by a member of management or an IT system administration delegate and only have the privileges necessary to function as required by the application, system, or database the account has been created for.
UA-1.2F	Network access is disabled within 24 hours of termination. Automated nightly processes disable access upon termination and initiate manager review on employee position changes, in accordance with Voya policies.
UA-2:	Access Control Management
UA-2.1	Voya maintains a comprehensive physical security program. Access to Voya facilities is restricted and logs are maintained for all access. Physical security and environmental controls are present in Voya buildings.
UA-2.2	Voya ensures that access to systems that access, process, store, or transmit Client PI is limited to only those personnel who have been specifically authorized to have access in accordance with the user's assigned job responsibilities.
UA-2.3	Voya ensures that accounts for systems that access, process, store, or transmit Client PI are controlled in the following manner:
UA-2.3A	Users must provide a unique ID and Password for access to systems. Access to applications/systems is limited to a need-to-know basis, and is enforced through role based access controls.
UA-2.3B	Accounts are protected on computing assets by screen-savers that are configured with an inactivity time-out of not more than 15 minutes.
UA-2.3C	Accounts are locked after no more than 10 consecutive failed logon attempts, depending upon the system and platform.
UA-2.3D	Accounts remain locked until unlocked by an Administrator or through an approved and secure end-user self-service process.
UA-2.3E	Accounts are reviewed on a periodic and regular basis (semi-annually for non-privileged and privileged accounts) to ensure that the account is still required, access is appropriate, and the account is assigned to the appropriate user.
UA2.4	Voya ensures that wireless mobile devices are secured against threats coming from these wireless networks and wireless connections are required to be encrypted.
UA-3:	User Access Management
UA-3.1	Voya ensures that passwords for all accounts on systems that access, process, store, or transmit Client PI are configured and managed as follows:

UA-3.1A	Passwords are stored using one-way encryption (e.g. cryptographic hash with a unique salt) in a secure file system or directory.
UA-3.1B	Passwords for all accounts have a minimum length of eight characters, a maximum age of 60 days for non-privileged accounts and 30 days for privileged accounts, and a password history equal to six or the maximum value allowed by the system.
UA-3.1C	Passwords have a complexity of at least one digit, one uppercase and one lowercase letter, contain no common words, and do not use a repetitive string of characters.
UA-3.1D	Initial passwords are different from the name of user account, communicated to users in a secure manner, and required to be changed the first time the user logs in.
UA-4:	Information Access Restriction
UA-4.1	Voya implements information access restrictions on all systems used to access, process, store, or transmit Client Information.
UA-4.2	Voya ensures the following Information Access Restrictions are in place:
UA-4.2A	Access to underlying operating systems and application features that the user does not require access to in the performance of their assigned responsibilities are strictly controlled.
UA-4.2B	Access to source code and libraries are restricted to only those individuals who have been specifically approved to have access. A person who develops code changes cannot be the same person who migrates the code change into production.
UA-4.2C	Access between Development, Test, and Production environments are strictly controlled. The version management system provides segregation of code, data and environments.
UA-4.2D	Temporary privileged access to production data is granted to authorized personnel based on job function for emergency support and only via access control and logging security tools.
PS:	Platform Security Controls
PS-1:	Computer System Security (Servers and Multi-user Systems only)
PS-1.1	Voya implements and manages a formal process for ensuring that all computer systems that access, process, store, or transmit Client PI are protected and configured as follows prior to and while remaining in a production status:
PS-1.1A	Systems are assigned to an asset owner within Voya's organization.
PS-1.1B	Systems are located in a data center or similarly controlled environment with appropriate physical security mechanisms and environmental controls to ensure systems are protected from theft, vandalism, unplanned outages, or other intentional or unintentional hazards.
PS-1.1C	All systems are configured to meet Voya standards, monitored to ensure a compliant state, and patched as required to maintain a high degree of security. Issues found to be out of compliance are required to be tracked to closure.
PS-1.1D	Systems are configured with commercially available and licensed anti-virus software which is set to perform active scans, perform scans of uploaded or downloaded data/files/web content, and is updated on at least on a daily basis.
PS-1.1E	System clocks are configured to synchronize with a reputable time source (e.g., NTP).
PS-1.1F	Systems display a warning banner to all individuals during the logon process that indicates only authorized users may access the system.
PS-1.1G	Systems that have been implemented into a production environment are routinely tested for vulnerabilities and risks using industry best practice tools and methods.
PS-1.1H	All high and medium vulnerability and risk issues identified are remediated utilizing a risk based approach and in alignment with application team code release schedules.
PS-1.1I	Voya ensures that only authorized and trained personnel have access to configure, manage, or monitor systems.
PS-2:	Network Security
PS-2.1	To ensure systems accessing, processing, storing, or transmitting Client PI are protected from network related threats, Voya implements the following network security controls prior to connecting any network component to a production network and for the duration that the component remains in a production status:

PS-2.1A	Networks are constructed using a defense-in-depth architecture, are terminated at a firewall where there are connections to external networks, and are routinely scanned for unapproved nodes and networks.
PS-2.1B	Business-to-Business (B2B) and Third Party network connections (Trusted) to systems accessing, processing, storing, or transmitting Client PI are permitted only after a rigorous risk assessment and formal approval by Voya management. Network connections from un-trusted sources to internal resources are not permitted at any time.
PS-2.1C	Network components (switches, routers, load balancers, etc.) are located in a data center or a secure area or facility.
PS-2.1D	Voya systems are configured to provide only essential capabilities and restrict the use of any unneeded functions, ports, protocols and services.
PS-2.1E	Intrusion detection/prevention technologies, firewalls, and proxy technologies are implemented, monitored and managed to ensure only authorized and approved traffic is allowed within and between segments of the network.
PS-2.1F	Internal Voya wireless networks are configured with the most robust security standards available, including but not limited to, 802.11i/n, strong authentication, IP/MAC address filtering, firewall protection, and intrusion detection/prevention.
PS-2.1G	Wireless networks are not used to access Client Information unless the information is encrypted at either the file or transport level.
PS-2.1H	Network components that have been implemented into a production environment are routinely tested for vulnerabilities and risks using industry best practice tools and methods.
PS-2.1I	Voya ensures that only authorized and trained personnel have access to configure, manage, or monitor network components.
PS-3:	Generic Application and Database Security
PS-3.1	Voya implements and maintains an application security certification and assurance process that ensures that all applications that access, process, store, or transmit Client PI provide the following:
PS-3.1A	Application and database design ensures security, accuracy, completeness, timeliness, and authentication/authorization of inputs, processing, and outputs.
PS-3.1B	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.
PS-3.1C	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.
PS-3.1D	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 of security.
PS-3.1E	Applications and databases are implemented into a production environment with minimal privileges and critical configuration files and storage subsystems are protected from unauthorized access.
PS-3.1F	Applications and databases that have been implemented into a production environment are routinely tested for vulnerabilities and risks using industry best practice tools and methods.
PS-3.1G	Voya ensures that Consumer/Internet facing applications have been designed and implemented using multi-factor authentication architecture. Web sessions require the use of an HTTPS (encrypted) connection, as well as authorization to approved data and services.
PS-3.1H	Voya ensures that only authorized and trained personnel have access to configure, manage, or monitor applications and databases.
PS-4:	Workstation and Mobile Devices Security (End User Devices)
PS-4.1	Voya ensures that the following security controls have been implemented and are maintained to protect Client PI accessed, processed, stored, or transmitted on workstations and mobile devices.

PS-4.1A	Workstations are located in a physically secure environment with mechanisms in place to prevent unauthorized personnel from accessing data stored on the device, reconfiguring the BIOS or system components, or from booting the device from unauthorized media. Portable devices are configured for boot-up encryption.
PS-4.1B	Laptops/portable computers and other mobile devices are assigned to an owner who is responsible for physically securing the device at all times, and the owner of the device must receive adequate awareness training on mobile device physical security.
PS-4.1C	Portable devices are configured for boot-up encryption. All laptop hard drives are encrypted using AES 256. Any device deemed "remote" requires hard drive encryption.
PS-4.1D	All workstations, laptops/portable computers and other mobile devices (where applicable) are configured with commercially available and licensed anti-virus software which is set to perform active scans, to perform scans of uploaded or downloaded data/files/web content, and is updated on at least a daily basis.
PS-4.1E	All workstations, laptops/portable computers and other mobile devices (where applicable) are configured with a commercially available and licensed operating system, patched according to manufacturer's recommendations, hardened according to best industry practices and standards and configured so that regular users do not have administrative privileges.
PS-4.1F	Laptops/portable computers and other mobile devices (where applicable) are configured with personal firewall technology.
PS-4.1G	All Client PI stored on a workstation, laptop/portable computer or mobile device is backed up to an alternate storage area.
PS-4.1H	Workstations, laptops/portable computers and other mobile devices (where applicable) display a warning banner to all individuals during the logon process that indicates that only authorized users may access the system or device.
PS-4.1I	Voya implements and maintains processes for recovering laptops/portable computers and mobile devices from terminated Voya Personnel.
PS-5:	Backup and Restore
PS-5.1	Voya implements and maintains backup and restore procedures to ensure that all Client PI received, disclosed, created, or otherwise in the possession of Voya is appropriately protected against loss.
PS-5.2	Voya ensures that backups are securely stored and storage systems are physically and logically protected.
PS-5.3	Voya implements a backup and availability schedule to meet business and regulatory requirements.
PS-6:	Remote Network Access Controls
PS-6.1	Voya implements and maintains a remote network access control strategy or process.
PS-6.2	Voya ensures the following remote network access controls are in place:
PS-6.2A	Users requiring remote access are appropriately authorized by Voya management.
PS-6.2B	Remote access connections are established through the use of Virtual Private Networking (VPN) or secure VDI mechanisms that provide transmission security, encryption and connection timeout (e.g. split-tunneling disabled.)
PS-6.2C	Only Voya- approved and controlled (managed) computing devices are used when remotely accessing (where applicable) Voya's computing environments where Client PI is held. Any device deemed "remote" requires data encryption. Encrypted communications are required for all remote connections.
PS-6.2D	Users are thoroughly authenticated using multi-factor authentication prior to being provided remote access.

ITR:	IT Resilience Controls
ITR-1:	Architecture
ITR-1.1	Voya ensures that the architecture of computing environments where Client PI is accessed, processed, stored, or transmitted incorporates reasonable industry best practices for authentication/authorization, monitoring/management, network design, connectivity design, firewall and intrusion prevention technologies and storage and backup capabilities.
ITR-2:	Hardware and Software Infrastructure Resilience
ITR-2.1	Voya ensures all hardware and software components classified with an availability rating of "critical" used in the accessing, processing, storage, or transmission of Client PI is: • Identified and cataloged • Supported by the manufacturer of the component (or if developed in-house, follows Voya's SDLC Policy which includes quality/security) • Applications and systems classified as A4 may be designed with high availability features and have no single point of failure • Reviewed on a regular basis for capacity implications (at minimum once every 12 months)
ITR-2.2	Voya maintains Business Continuity Plans to address business unit and departmental actions to be undertaken before, during and after an incident or disaster. Voya's Disaster Recovery Plan addresses the recovery and availability of systems and data.
ITR-3:	Capacity Assurance
ITR-3.1	Voya ensures that computing environments used to access, process, store, or transmit Client PI are assessed for capacity and performance on a periodic basis (at minimum once every 12 months) and appropriate corrective actions are taken to make the environment sufficiently robust enough to perform its stated mission.
CM:	Change Management Controls
CM-1:	Change Management Process
CM-1.1	Voya implements and maintains a change control process to ensure that all changes to the environment where Client PI is accessed, processed, stored, or transmitted is strictly documented, assessed for impact, approved by personnel authorized by Voya to provide approval for such changes, thoroughly tested, accepted by management, and tracked.
CM-1.2	Voya implements an emergency change control process to manage changes required in an emergency situation where a computing system is down or there are imminent threats/risks to critical systems involving Client PI.
CM-2:	Separation of Environments
CM-2.1	Voya maintains physically and/or logically separate development, test, and production computing environments. Development, testing, and acceptance environments are separate from the production environment.
CM-2.2	Voya ensures that Client data used for development or testing purposes is completely depersonalized/desensitized of confidential values prior to entering a development or test environment. Data is depersonalized in non-production controlled environments for testing purposes with required approvals. PI elements are required to be depersonalized in non-production environments.
SM:	Security Monitoring Controls
SM-1:	Security Event Monitoring and Incident Management
SM-1.1	Voya implements and maintains a security event monitoring process and associated mechanisms 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 Client PII.
SM-1.2	Voya implements and maintains an incident management process to ensure that all events with a potential security impact are identified, investigated, contained, remediated, and reported to Client effectively and in a timely manner.

SM-1.3	Voya has implemented monitoring controls that provide real-time notifications of events related to loss of confidentiality, the integrity, or the availability of systems.
SM-1.4	Event logs (audit trails) are stored for analysis purposes for a minimum period of 90 days.
SM-2:	Technical State Compliance
SM-2.1	Voya ensures computing environments that access, process, store, or transmit Client PII are continually in compliance with quality and security requirements including, but not limited to, authentication/authorization, monitoring/management, network design, connectivity design, firewall and intrusion prevention technologies, and storage and backup capabilities.
SM-2.2	Voya ensures IT Risk Management facilitates risk assessments of information technology processes and procedures in accordance with the annual IT Risk Assessment Plan approved by the IT/Privacy Risk Committee. Risk Assessment results are communicated to management for awareness and resolution or risk acceptance of findings based on management's risk appetite.
SM-3:	Security and Penetration Testing
SM-3.1	Voya implements and maintains vulnerability and penetration testing (Ethical Hacking) processes to ensure the computing environment where Client PII is accessed, processed, stored, or transmitted is continually protected from internal and external security threats.
SM-3.2	Voya implements and maintains a process for vulnerability scanning on at least a monthly basis and ensures issues are remediated utilizing a risk based approach within a reasonable timeframe.
SM-3.3	Penetration testing (Ethical Hacking) of Internet facing systems or systems exposed to un-trusted networks is conducted prior to the system being deployed into a production status, after any significant changes, and then at least once every 12 months thereafter.

EXHIBIT D

SELF-DEALING TRANSACTION DISCLOSURE FORM

In order to conduct business with the County of Fresno (hereinafter referred to as "County"), members of a contractor's board of directors (hereinafter referred to as "County Contractor"), must disclose any self-dealing transactions that they are a party to while providing goods, performing services, or both for the County. A self-dealing transaction is defined below:

"A self-dealing transaction means a transaction to which the corporation is a party and in which one or more of its directors has a material financial interest"

The definition above will be utilized for purposes of completing this disclosure form.

INSTRUCTIONS

(1) Enter board member's name, job title (if applicable), and date this disclosure is being made.

(2) Enter the board member's company/agency name and address.

(3) Describe in detail the nature of the self-dealing transaction that is being disclosed to the County. At a minimum, include a description of the following:

   a. The name of the agency/company with which the corporation has the transaction; and

   b. The nature of the material financial interest in the Corporation's transaction that the board member has.

(4) Describe in detail why the self-dealing transaction is appropriate based on applicable provisions of the Corporations Code.

(5) Form must be signed by the board member that is involved in the self-dealing transaction described in Sections (3) and (4).

(1) Company Board Member Information:			
Name:		**Date:**	
Job Title:			
(2) Company/Agency Name and Address:			
(3) Disclosure (Please describe the nature of the self-dealing transaction you are a party to):			
(4) Explain why this self-dealing transaction is consistent with the requirements of Corporations Code 5233 (a):			
(5) Authorized Signature			
Signature:		Date:	