Great-West Life & Annuity Insurance Company

AMENDMENT NO. 5
TO
AGREEMENT FOR RECORDKEEPING AND COMMUNICATION SERVICES

TULARE COUNTY

§457(b) Deferred Compensation Plans

Group No. 88038-01

And

§3121 Plan
Group No. 88038-02

THIS AMENDMENT is entered into by and between Great-West Life & Annuity Insurance Company or one of its affiliates, including Great-West Life & Annuity Insurance Company of New York, FASCore, LLC, and Great-West Financial Retirement Plan Services, LLC ("Empower" or "Empower Retirement"), and/or any successor or assign, and County of Tulare ("Plan Sponsor") with respect to the recordkeeping services provided by Empower to the 457(b) Deferred Compensation Plan ("457(b) Plan") group nos. 88038-01 and 88038-02, Plan (hereinafter referred to as the "Plan" or "Plans").

WHEREAS, Empower and Plan Sponsor have entered into an agreement for recordkeeping and communication services ("Agreement"), as amended, under which Empower provides certain recordkeeping and communication services for the Plan Sponsor with respect to the Plan; and

WHEREAS, Empower and Plan Sponsor have decided to amend the Agreement with respect to information security and privacy;

NOW, THEREFORE, in consideration of the covenants and conditions herein contained, and other good and valuable consideration as herein provided, the parties amend the Agreement as follows:

1. The Agreement is hereby amended by adding the attached Information Security and Privacy Exhibit, describing Empower's information security and privacy practices and commitments.

2. In all other respects, the Agreement shall remain in full force and effect.

3. This Amendment shall take effect on such date as it has been signed by both Plan Sponsor and Empower (the "Effective Date").

IN WITNESS WHEREOF, the parties, by signing this Amendment, certify that they have read and understood it, that they agree to be bound by its terms and that they have the authority to sign it. This Amendment is not binding on either party until signed by both parties.

TULARE COUNTY AGREEMENT NO. 25245-E

Important Note: Service Agreement Amendments, Pricing Change Agreements, and other contractual documents must be duly executed by both parties prior to the effective date of the changes. Backdating contracts or funding agreements is in violation of our corporate governance and regulatory requirements. Changes cannot be implemented prior to the date all documents are fully executed, even if that requires the effective date to be postponed. There are no exceptions to the rule that the effective date must follow the date all documents are executed.

COUNTY OF TULARE

BY _____ Date: 4-2-19

Name: KUYLER CROCKER (print name)
Chairman, Board of Supervisors
"Plan Sponsor"

ATTEST: _____
Jason T. Britt
Administrative Officer/Clerk of the
Board of Supervisors of the County of Tulare

By _____
Deputy Clerk

BOARD OF SUPERVISORS · TULARE COUNTY, CAL. ·

GREAT-WEST LIFE & ANNUITY INSURANCE COMPANY

BY _____ Date: 12/5/18
Daniel A. Morrison

TITLE: Senior Vice President, Government Markets
"Great-West"

Approved as to Form:
County Counsel

By _____ Date 12/11/18
Jennifer M. Flores
Chief Deputy County Counsel

INFORMATION SECURITY AND PRIVACY EXHIBIT

1. GENERAL DESCRIPTION AND DEFINITIONS

Under the terms of the Agreement, Empower and its affiliates are to provide recordkeeping, administrative, and other ministerial services to the Plan. In providing such services, Empower has deployed numerous technologies, procedures, and personnel to protect its internal recordkeeping system. Empower employs a layered approach with respect to its security features utilized for protecting Plan and Participant data as set forth herein. Empower reserves the right to make modifications to its technology and procedures that are designed to improve its information security protections and to conform to advances in technology and applicable industry standards. Empower's current cyber security program aligns to the industry standard published by the International Organization for Standardization (ISO 27001/27002), as well as to Federal, State and regulatory requirements.

This Exhibit shall be subject to, and shall incorporate by reference, the terms and conditions set forth in the Agreement. For purposes of this Exhibit, all defined terms shall have the same meaning as under the Agreement unless otherwise defined herein.

"Access Controls" shall mean the collection of mechanisms that specify what Empower personnel can do on its internal recordkeeping system, such as what resources Empower personnel can access and the operations such personnel can perform.

"Application Development Security" shall mean the security controls to be included in the system development process including, but not limited to application security controls, change and configuration control, data warehousing, data mining, knowledge-based systems, program interfaces, and the concepts used to help ensure software and overall system confidentiality, integrity, and availability.

"Cryptography" addresses the principles, means, and methods of disguising information to provide confidentiality, integrity, and availability.

"Information Security Program" shall mean the identification of Empower's information assets and the development, documentation, and implementation of written information security policies, standards, procedures, and guidelines, which ensure their availability, integrity, and confidentiality.

"Network Security" includes the provisions made in an underlying computer network infrastructure, policies adopted by the network administrator to protect the network and the network-accessible resources from unauthorized access, and consistent and continuous monitoring and measurement of its effectiveness (or lack) combined together.

"Operations Security" identifies the controls over hardware, media, and the personnel and administrators with access privileges to these resources.

"Physical Security" shall mean the physical environment surrounding the internal recordkeeping system and components.

"Risk Management" shall mean the identification, measurement, control, and minimization of loss associated with uncertain events or risks. It includes overall security reviews, risk analysis, evaluation and selection of safeguards, cost/benefit analysis, management decisions, safeguard implementations, and effectiveness reviews.

"Security Testing" means the system and application vulnerability assessments and external Internet application and infrastructure vulnerability assessments on all Empower systems used to provide the Services.

2. INFORMATION SECURITY PROGRAM & TRAINING

Empower's Information Security Board is responsible for the development, implementation, and ongoing maintenance of its Information Security Program. Empower furthers its Information Security Program through its implementation of documented IT control standards, written information security policies regarding data and information classification, security awareness training, and risk assessment and management, as set forth by the Information Security Board.

In connection with its Services and as part of its Information Security Program, Empower maintains stringent information security practices which mandate the secure protection and handling of Participant data. Empower personnel must complete initial security training at the time they are first employed with Empower and annually thereafter. All personnel attest annually to Empower's Code of Business Conduct and Ethics, which enforces the tenets of Empower's Information Security Policies.

In addition, Empower will monitor, evaluate, and adjust, as appropriate, its Information Security Program in light of relevant changes in Services, technology or industry security standards, the sensitivity of data collected or processed by Empower in the provision of its Services and evolving internal or external risks.

3. ACCESS CONTROL SYSTEMS AND METHODOLOGY

Empower utilizes Access Controls designed to ensure that only Empower personnel with the proper need and authority can access its internal recordkeeping system, are allowed to execute programs, and can read, edit, add and delete information. Empower's Access Controls may include but are not limited to: (i) limiting access to personnel with a requirement to view Participant data; (ii) establishing least-privilege controls to protect systems and Participant data; (iii) generation of audit trails, including logging of changes to Participant data by recording details such as the date, time and ID of the Participant or personnel making the change; (iv) minimum length and complexity requirements for passwords for Empower personnel and Participant accounts; (v) periodic review and approval of personnel need to access the Empower recordkeeping system; and (vi) termination of personnel access promptly following severance from employment.

4. CRYPTOGRAPHY

Empower uses Cryptography techniques that assist Empower with preventing the unauthorized capture, modification of or access to data or information while stored on the Empower recordkeeping system or accessed by Empower personnel. Such Cryptography techniques may include but are not limited to: (i) encryption of sensitive data sent across external communication lines; (ii) requirement of minimum 128-bit encryption SSL encryption for web browsers; and (iii) encryption of Empower data while stored on laptops and mobile devices. Empower uses standard encryption algorithms that follow up-to-date encryption standards and industry practices.

5. OPERATIONS SECURITY

Operations Security is employed for purposes of safeguarding information assets while the Plan and Participant data is resident in the recordkeeping system, storage media, or otherwise associated with the data processing environment. Operations Security includes but is not limited to: (i) personnel workstations are protected by user profiles with anti-virus programs; (ii) implementation of firewall protection, router configuration rules and standards designed to maintain the integrity of Participant data; (iii) restriction of connections and communications with untrusted networks, and (iv) actively monitoring the network perimeter, including intrusion detection systems, for attempted intrusions.

In addition, Empower's Information Security Program mandates ongoing Operations Security requirements, including but not limited to, installing or maintaining (i) security patches for operating systems and applications within standard timeframes based on severity, (ii) industry standard versions of operating systems, software and firmware for system applications and components and (iii) up-to-date system security agent software which includes updated malware and virus definitions. In all of the foregoing instances, Empower reserves the right to conduct pre-installation testing and to determine whether and to what extent such patches or updates are reasonable and will not introduce new and/or unacceptable risks to Empower's systems, processing environment or data.

6. PHYSICAL SECURITY

Physical Security includes but is not limited to (i) physical security in the protection of valuable information assets of the business enterprise; and (ii) providing protection techniques for the entire facility, from the outside perimeter to the inside office space, including the datacenters and wiring closets.

Physical Security is applied to datacenters as follows: (a) highly-secured and substantially redundant configurations to help ensure continuity of operations; (b) access is controlled using key cards and monitored with use of extensive camera systems; (c) access is removed in a timely manner upon termination or reassignment and access is reviewed and recertified regularly; (d) visitors must be pre-approved for access

and physically escorted while in the datacenter; (e) 24x7 monitoring of environmental controls and physical security is in place; and (f) security is routinely tested by both internal and external auditors.

7. SECURITY TESTING

In connection with its Services hereunder, Empower will conduct the following Security Testing: (i) test information technology general controls (ITGC) at least annually or whenever there is a material change in business practices, and (ii) conduct infrastructure penetration tests and scans against Internet-facing points of presence. Empower will correct vulnerabilities or security issues discovered through such assessments in a manner and time frame consistent with established standards.

8. INVESTIGATIONS AND INCIDENT RESPONSE

In connection with its Services hereunder, Empower has investigative measures and techniques for incident handling including but not limited to: (i) a formalized, enterprise-wide Computer Security Incident Response Team ("CSIRT"); (ii) CSIRT processes which are tested at least annually; and (iii) periodic validation of CSIRT processes by Empower's internal audit group.

Empower will notify Plan Sponsor within 60 days after becoming aware of any security breach that has compromised the security, confidentiality or integrity of Plan Sponsor's data and resulted in unauthorized access to Plan Participant data by a third party (collectively any "Information Security Incident"). In the event of an Information Security Incident, Empower will: (i) investigate and assist any regulator or other governmental body with oversight over the Information Security Incident in investigating, remedying and taking any other action regarding the Information Security Incident as appropriate or required by law; (ii) provide Plan Sponsor with information about remedial measures have been undertaken to prevent such Information Security Incident from reoccurring. Empower will provide Plan Sponsor with periodic Information Security Incident status updates and a final report once the Information Security Incident has been resolved.

9. GLOBAL DATA PROCESSING

Where Empower will receive and/or facilitate the exchange of data and information of individuals under Plan Sponsor's Plan (as defined in the Services Agreement, the "Participants") originating in a European Union member country ("Personal Data"), Empower represents that, to the extent it processes the Personal Data in the United States, the following terms shall apply:

- Empower agrees to comply with all data protection laws applicable to Empower's Services. Plan Sponsor, as data controller, authorizes Empower to process the Personal Data for the purposes set out in the Services Agreement.

- Plan Sponsor warrants to Empower that:

    - it has all necessary rights to authorize Empower to process Personal Data in accordance with the Services performed by Empower under this Agreement and applicable data protection laws; and

    - its direction to Empower relating to processing of Personal Data will not put Empower in breach of applicable data protection laws.

- Empower represents that it currently does the following, and warrants to continue to do the following:

    - process the Personal Data in furtherance of the purposes as set forth in the Services Agreement in a manner so as to maintain the accuracy and integrity of such Data in the form received;

    - maintain a privacy disclosure for all Empower web sites and portals to be used by individuals that collect Personal Data other than a user name and password which meets the following requirements - a privacy disclosure that includes in clear and conspicuous language when individuals are first asked to provide Personal Data to Empower or as soon thereafter as is practicable (i) identifying Empower as the organization collecting, processing and safeguarding the Personal Data on behalf of the Plan; (ii) outlining the permissible purpose(s) of Empower processing of Personal Data; (iii) furnishing information regarding

the choices/means Empower offers the individual(s) for limiting the use and disclosure of their Personal Data; and (iv) including Empower representatives' contact details to which queries or complaints can be addressed;

- utilize cookies solely as set forth in the privacy disclosure;

- take reasonable steps to ensure the reliability of any Empower personnel who have access to Personal Data and ensure that any personnel authorized to process Personal Data (i) are subject to contractual confidentiality obligations consistent with those set out herein or are under an appropriate statutory and/or regulatory obligation of confidentiality; and (ii) comply with the obligations of this Section;

- not publish, disclose or divulge any Personal Data to a third party unless such is required to provide the Services pursuant to the Agreement and as otherwise set forth in the Services Agreement;

- identify the minimum Personal Data set required to provide the Services, and other legitimate business purposes as authorized by Plan Sponsor or the Participant (or where permissible under applicable law or regulation to the extent not prohibited by any such authorization) and ensure the Personal Data processed is limited to this minimum set;

- ensure Personal Data that Empower holds is able to be corrected, amended or deleted where Empower determines the information is inaccurate, or has been processed in violation of this Agreement and/or applicable law or regulation, provided that in the event of conflicts of laws, Empower may make a reasonable determination as to the deletion of data to comply with the laws most applicable to the Services;

- if Empower receives notice from Plan Sponsor or a Participant who has accessed the Services that unauthorized processing by Empower personnel has occurred, or if Empower makes a determination that it can no longer meet its obligations to provide the level of protection required by this clause, take prompt, reasonable and appropriate steps to stop and remediate the unauthorized processing and inform Plan Sponsor of all such actions in writing, or to terminate, upon reasonable notice to Plan Sponsor, that portion of the Services that may be deemed to constitute unauthorized processing. Empower agrees to provide reasonable cooperation to Plan Sponsor to respond to any inquiries regarding practices related to the collection, use, and disclosure of Personal Data in connection with this Agreement or any requests to access and correct Personal Data by or on behalf of Participants; and

- return to Plan Sponsor all Personal Data held by Empower after the end of the provision of Services and securely delete any remaining copies. Notwithstanding the foregoing, Empower will be permitted to retain any Personal Data which it has to keep to comply with any applicable law or which it is required to retain for insurance, accounting, taxation or record keeping purposes, or that is otherwise impracticable to delete. This **Exhibit** will continue to apply to retained Personal Data until such data is destroyed.