ANTI-MONEY LAUNDERING PROGRAM
Applicable to:

Athene USA (the Company)

1 Purpose

a) This program is designed to comply specifically with the requirements of the Bank Secrecy Act (as amended by the USA PATRIOT Act, Pub. Law 107-56 [2001]), and any other related federal or state law or regulation that may apply. It is designed to provide a mechanism to detect, investigate, and report suspected money laundering, sanction violations and/or other Financial Crimes to the Department of Treasury, Office of Foreign Assets Control (OFAC) and/or Financial Crimes Enforcement Network (FinCEN).

b) Criminal activities, including terrorist financing activities, may be financed through reverse money laundering, that is, using legitimate sources of funds to support illegal activity.

c) The Company will support Anti-Money Laundering (AML) laws by adopting and implementing the following principles:

i) The issuance of risk-based written policies, procedures, and internal controls to identify and report money laundering, including procedures to cover the obtaining of relevant customer-related information, and the integration of the company's insurance producers and brokers into these procedures;

ii) The designation of a compliance officer responsible for the implementation, monitoring and updating of the program, and training;

iii) Providing for ongoing training of appropriate persons concerning their responsibilities under the program;

iv) Providing for independent testing to monitor and maintain an adequate program.

2 Definition of Money Laundering

a) Money laundering occurs when someone uses legitimate financial mechanisms, including insurance products, to make the proceeds of his or her illegal activity appear legitimate by attempting to conceal or disguise the nature, location, source, ownership, or control of illegally obtained money. Money laundering schemes will include one or more of the following activities:

i) **Placement** involves physically placing illegally obtained money into the financial system (that is, conversion of illegal funds into monetary instruments, such as traveler's checks or money orders, deposited into accounts at financial institutions). Money is most vulnerable to detection and seizure during placement. One example in which the insurance industry may experience placement is an attempt by the customer to pay premiums, generally large amounts, from cash, using cashier's checks, multiple money orders and/or any combination thereof.

ii) **Layering** involves separating the illegally obtained money from its criminal source by completing a series of financial transactions (that is, transferring funds into other accounts or other financial institutions), which makes it difficult to trace the money back to its original source. For example, a customer may use multiple sources such as wire transfers, personal checks, and 1035 exchange funds to establish or add to an annuity contract.

iii) **Integration** involves moving the proceeds into a seemingly legitimate form. The funds are reintroduced into the economy and used to purchase legitimate assets (automobiles, real estate, jewelry, etc.) or to fund other criminal activities or legitimate businesses. This can be evidenced by the use of a variety of forms of payments to achieve a maximum cash value and immediately taking a loan or canceling/free-look of a policy/contract for the purchase of an asset such as a car, business, or home.

iv) **Structuring** is the act of breaking up a potentially large transaction into several smaller ones. It is illegal to structure transactions in order to avoid recordkeeping or reporting requirements. Likewise, it is illegal to assist anyone in structuring transactions in order to avoid recordkeeping or reporting requirements. For example, an associate may not tell or even imply to a customer that the customer can avoid providing information by conducting a transaction involving a smaller amount of money.

3 Company Policy Against Money Laundering

a) The Company does not support, and will not knowingly assist, in any activity which facilitates money laundering or the funding of terrorist or criminal activities. The Company is committed to compliance with laws and regulations designed to combat money-laundering activity.

b) Officers, employees and producers should demonstrate behavior in the performance of their jobs aligned with this Policy and the Anti-Money Laundering Program. Associates must understand that it is the policy of the Company to comply with all laws, regulations, and Company guidelines that apply to the business of the Company and to, wherever possible, prevent the occurrence of money laundering activities. Associates are expected to follow and adhere to all policies and procedures with the understanding that not doing so may lead to disciplinary action, up to and including termination.

4 Compliance Officer

a) The Compliance Officer for the Company's AML Program is the Senior Vice-President and Chief Compliance Officer (CCO) for the Company. S/he is appointed by the Board or executive officer at the direction of the Board.

b) The CCO or his/her designee is responsible for implementation, monitoring, and enforcement of the day-to-day operations, internal controls, training program, and all other activities relating to the Company's AML Program.

c) The CCO may delegate specific functions, including the responsibility for implementing and monitoring the day-to-day operations, internal controls, the training programs, and all other activities relating to the Company's AML program.

d) The CCO or his/her designee will make available on an ongoing basis this program and information affecting this program to all interested parties, including but not limited to officers, home office associates (employees), senior management, and producers, in a manner and format deemed appropriate by the CCO or his/her designee. The CCO or his/her designee will update such parties on an ongoing basis about the status of, and any changes to, this program.

e) The CCO or his/her designee will take steps necessary to maintain expertise in anti-money laundering techniques, including participating in educational training, attending seminars, and reading articles and journals or other information as deemed necessary and appropriate. The CCO or his/her designee will ensure that other Compliance Analysts with responsibilities for AML activities also maintain a level of expertise through the same appropriate methods.

5 Know Your Customer (KYC)

a) Identification Verification of the Applicant/Owner.

i) The obtaining of relevant information about a customer is a critical part of the Company's AML Program. The Company has developed and implemented its own KYC requirements.

b) Notice to Customers of Identify Verification Requirements

i) The Company has opted to provide customers with adequate notice that it will request documentation to verify their identity. Notice is adequate when it gives a general description of the identification requirements and is provided before opening the account. The Company will provide notice to the customer via the Authorization and Acknowledgement section of the application. Additionally, identification requirements will be posted on the Company's internal websites for associate access.

c) Identification of Applicant/Owner

i) The application and all accompanying documents and other pertinent information gathered should be reviewed to the extent reasonable and practicable to determine and verify the true identity of any customer seeking to purchase an insurance or annuity product with the Company. Any information used to form a basis of identification will be maintained for a minimum of (5) years (unless local regulations stipulated a longer period) from the date the customer/entity relationship has ended. The CCO or his/her designee should be notified of any irregularities or questions regarding the identification of the applicant.

ii) All customers will be required to provide certain specific information in order for us to make a determination of identification. No contract will be processed without our first having received this information. Any application received without this complete information will be held and not processed until either the information is received, or until the application is returned per the Company's processes for incomplete applications.

(1) Information required from individuals:

(a) full name (first, middle initial, last);

(b) current physical (not P.O. Box) street address, city, state, and zip;

(c) current physical (not P.O. Box) business street address, city, state, and zip if applicable;

(d) Social Security Number or Tax Identification Number;

(e) date of birth;

(f) an officially issued identification document such as a passport, driver's license, or United States visa; if a Foreign National Card is received, identity must be compared to the Specially Designated Nationals list;

(g) the serial number or other identification number associated with that document;

(h) the place where that document was issued;

(i) the date the document was issued; and

(j) the date the document expires.

(2) Information required from legal entities:

(a) The full name and address of the entity (excluding P.O. Boxes);

(b) The jurisdiction of formation and legal form of the entity;

(c) The Social Security Number or Taxpayer Identification Number;

(d) The names of all persons with responsibility for the management of the affairs of the entity (directors, general partners, trustees, authorized signatories), or copy of its annual statement.

(e) Information about beneficial ownership. Athene is required to identify everyone who, directly or indirectly, owns 25% or more interest, e.g., shares of stock in a corporation or membership interests in a limited liability company, of a legal entity. Athene is required to identify where an applicant is acting as a producer on behalf of another, and, in the case of trusts, also obtain information about the settler(s) and any persons or entities that have control over the funds or the power to remove trustees.

(f) Copies of documents providing the existence of the entity (e.g., certificate of incorporation, memorandum and articles of association, trust deed, partnership agreement, or a certificate of good standing); any beneficial owner(s) must be identified.

(g) Current list of authorized signatories or copies of power of attorney to establish and document that the entity's representative(s) are authorized to act on the entity's behalf.

iii) Additional due diligence may be warranted depending on the specific circumstances, including the type of applicant, the applicant's home jurisdiction and how well the producer and Company already know the applicant. Additional due diligence may include, for example, reviewing negative news and databases to determine criminal, civil or regulatory proceedings against an applicant, producer and/or taking steps to ensure that the applicant, or the source of the funds, is legitimate.

iv) Any associate who determines that the required information is not provided should notify his or her supervisor or manager. The manager should verify that all attempts to gather the information have been made. If the information is still missing, the manager should report the lack of information to the CCO or his/her designee through the means provided in the Company's Anti-Fraud Guidelines.

v) The Company may also utilize a non-documentary verification process. This process could include making direct customer contact; independent verification of the customer's identity by comparing information given by the customer with information obtained from a consumer credit report agency, public database or other source; checking references with other financial institutions; or obtaining the customer's financial statement. The Company's procedures for non-documentary verification will take into consideration situations where an individual is not able to provide current government-issued identification documents with a photo or other safeguard or where the producer is unfamiliar

with the documents presented by a customer. The application will be assigned to a "pended" status until the information is verified.

d) OFAC (Office of Foreign Asset Control) / HM (Her Majesty) Reviews

i) Applications and claims will be reviewed prior to the providing of service to determine whether any party to the transaction, including the insured, owner, beneficiary, premium payor or bank, appears on any of the OFAC/HM sponsored lists of blocked persons and/or sanctioned countries. The CCO or his/her designee shall be responsible for investigating and taking appropriate actions concerning potential OFAC/HM matches, consistent with the Company's OFAC/HM procedures.

ii) All new or changed information entered into the administrative systems will be reviewed periodically against the OFAC/HM sponsored lists in compliance with the Company's OFAC/HM procedures. In addition, a quarterly sweep is also completed.

6 Policies, Procedures and Controls – Monitoring and Detection

a) Policy and Controls

i) As the types of transactions that may be used by a money launderer are almost unlimited, it is difficult to define a suspicious transaction. However, a suspicious transaction will often be one that is inconsistent with a customer's known, legitimate business or personal activities or that is inconsistent with the normal course of business for a life insurance or annuity contract purchase. The Company's products that may be subject to money laundering would be permanent life insurance (not group life), annuity contracts (not group annuities), and any other insurance product having cash value.

ii) The Company maintains a risk-based approach to AML. Risks may be identified at different stages of a relationship, and the risk may also change as the relationship develops; therefore, relationships are monitored for change in order to react accordingly. The Company's structure for assessing risk is divided into two components.

(1) **Identifying primary drivers** which determine risk at the commencement of the relationship as follows:

(a) Customers
(b) Transactions
(c) Geographies

(2) **Monitoring** the primary drivers and measuring the effectiveness of the controls engaged to mitigate risk.

iii) The Company will monitor through automated means, where appropriate and reasonable, and through the use of manual means where necessary and expedient. The following internal controls are in place to assist those affected employees in the detection and prevention of money laundering activities. The business units identified as having the highest potential for discovering and incidence of suspected money laundering are New Business and In-Force. However, all business units and employees would be familiar with this program and the established controls.

(1) Cash and Cash Equivalents

(a) Cash payment of premiums is not allowed.

(b) Payment of premiums by cash equivalents such as Travelers Checks is not allowed.

(c) Payment of premium by Money Orders is not allowed. The only exception is the closed blocks of business administered by the Company's third-party administrators (TPA). When a Money Order is received by the TPA, the following conditions must be met:

i. The Know Your Customer requirements have been met satisfactorily;
ii. The Money Order was purchased by the applicant; and
iii. The Money Order amount is under $1,000.

(d) Payments by Cashier's Check are not encouraged. However, in the event a Cashier's Check is submitted, it must be drawn from the remitter's U.S.A. bank account with the owner listed as the remitter.

(e) Excessive premium payments attempted by cash or cash equivalents will be reviewed upon discovery or at a minimum monthly by the CCO or his/her designee. These payments will be reviewed to determine if there is any suspicious activity related to the case file. The CCO or his/her designee will report any applicable transactions as required by regulatory officials via a SAR. SARs will be reported immediately upon completion of an investigation, but not more than 30 days from the date of the premium receipt.

(2) Premium Checks

(a) Premium checks received are reviewed at the time of receipt and prior to processing for adherence to the Forms of Payment guidelines. Unacceptable forms of payment are marked as such and communicated to the New Business or In-Force area for resolution. If the issuing bank, payor and/or address of payor appear to be suspicious, the issue should be brought to the attention of the Compliance Department using the Request for Compliance Review form.

(b) Starter or temporary checks are not an acceptable form of payment and should not be accepted. When presented with this form of payment, associates and/or producers must refuse and inform the customer of the appropriate form of payment as identified in the standards set forth in the Forms of Payment. When there are repeat attempts of paying via starter or temporary checks, associates and/or producers must report the incidence to the Compliance Department using the Request for Compliance Review form. The payment should be returned, and the customer informed of the appropriate form of payment. An exception to this rule is if a starter check is from an account owned by a trust and the trust is the owner of the contract. Many times, trust accounts are established solely for the purpose of contributing to an annuity contract. After a due diligence review of the file to identify if any additional red flags exist, the payment may be accepted on a <u>one-time</u> basis.

(c) The Company does not authorize producers to accept premium checks payable to any person or entity other than one of the Athene USA Companies. No producer checks are permitted for the payment of premiums, except in cases where the producer is the applicant or annuitant. Unless the producer is the applicant or annuitant, any checks drawn on a producer's account should be referred to the Compliance Department via the Request for Compliance Review, and then returned to the producer with an explanation. The contract owner should also be notified.

(d) Special attention should be made in any attempt by the customer to pay initial or recurring premiums via a third-party person or entity not associated with the contract owner.

(3) Wire Transfers (New Business/Inforce)

(a) For cases in which the premium is paid by wire transfer, the originator of the wire transfer shall be identified. The Manager of the New Business Department should be notified of any suspicious activity regarding the transfer. Where the producer is the originator of the wire transfer, except in those instances when the producer is the customer/applicant/annuitant, the CCO, or his/her designee, shall be notified using the Request for Compliance Review. Wire transfers in excessive amount (outside the normal requirements of the case file) should be reported to the Compliance Department via the Request for Compliance Review form.

(b) Wire transfers or payments are made to or from unrelated third parties (foreign or domestic), or where the name or account number of the beneficiary or remitter has not been supplied. Where a third party is the originator of the wire transfer, the CCO, or his/her designee, shall be notified using the Request for Compliance Review.

(4) Foreign Persons/Foreign Funds

(a) Definition: A foreign person includes a nonresident alien individual, a foreign corporation, a foreign partnership, a foreign trust, a foreign estate, and any other person that is not a U.S.A. person.

(b) The Company will only issue contracts to foreign nationals as defined by and in accordance with the Guidelines for Writing Annuity Business on Foreign Nationals. Please refer to the Doing Business with Athene Producer Guide. The Company will not transact business with a foreign corporation, foreign partnership, foreign trust or foreign estate of an OFAC/HM sanctioned or prohibited countries.

(c) The Company will not accept foreign currency, or premium payments from banks or entities located in foreign countries identified as OFAC/HM sanctioned countries. These payments should be brought to the attention of the CCO or his/her designee via the Request for Compliance Review form and may be subject to the blocking/freezing of assets.

(d) If an account is opened by a politically exposed person (PEP), particularly in conjunction with one or more additional risk factors, such as the account being opened by a shell company beneficially owned or controlled by the PEP, the PEP is from a country which has been identified by FATF as having strategic AML regime deficiencies, or the PEP is from a country known to have a high level of corruption, an enhanced review will occur by the Compliance Department.

(5) Authority (In-Force)

Policy service requests will be reviewed to determine that the person making the request has the authority to do so. Special attention should be given to requests made by a power of attorney, trustee or other third party on behalf of the contract owner. The department supervisor or manager should review any unusual or irregular requests and should report those to the Compliance Department via the Request for Compliance Review form.

(6) Address Changes (In-Force and Mail Room)

(a) Written requests to change the address of record for the contract owner should be in writing and signed and dated by the contract owner. If a request is received in any other form, the Company will verify that the owner has made the request through use of various means of identifying the owner such as requesting the owner's social security number, tax identification number, address, or birth date before making the change. Notification of a

change in address received from an authoritative source, such as the United States Postal Service, will also be accepted. Any request to change the permanent street address to a Post Office Box (P.O. Box) will not be allowed.

(b) If we receive a request to change an address to an OFAC/HM sanctioned country, the request shall be forwarded to the CCO or his/her designee or Compliance Analysts by completing and submitting the Request for Company Review form.

(7) Ownership and Beneficiary Changes (In-Force)

(a) Ownership and beneficiary changes must be submitted in a manner acceptable to the Company. All such requests must be properly executed and dated by the contract policy owner of record. Beneficiary changes should be verified by letter to the contract owner. Ownership changes shall be verified by letter to the new contract owner. Signatures should be reviewed, and any discrepancy brought to the attention of the Compliance Department.

(b) Owner and beneficiary changes are reviewed to determine whether the designated owner or beneficiary is identified on any of the OFAC/HM lists. All parties to the transaction must be reviewed to determine if they are from an OFAC embargoed country or a specially designated person. The CCO, or his/her designee, shall be responsible for investigating and taking appropriate action concerning potential OFAC matches, consistent with the Company's OFAC procedures.

(c) Owner or beneficiary changes will be recorded in the administrative system and reviewed against the OFAC/HM sponsored lists on a daily basis in compliance with the Company's OFAC/HM procedures. In addition, the data will be compared quarterly to the OFAC/HM sponsored lists.

(8) Withdrawal / Surrender Requests / Loans (In Force)

(a) Requests for partial withdrawals, surrenders, or loans will be reviewed to determine that the person requesting the transaction has the authority to do so and that payments are not made to individuals or entities appearing on the OFAC/HM sanctioned lists or from an OFAC/HM sanctioned country.

(b) Any withdrawal, surrender, or loan request of any amount where the funds are to be wired or sent to a third-party or to another firm without any apparent business purpose must be approved by the Compliance Department via the Request for Compliance Review. This does not apply to a surrender relating to a Section 1035 exchange. If money laundering or other fraud is suspected, the Department supervisor or manager should be notified for further review and investigation.

(c) Withdrawal, surrender, and loan checks are reviewed for OFAC/HM compliance consistent with the Company's OFAC/HM program.

b) Suspicious activity relating to New Business / Policy and Contract Opening

i) The following are examples of activity that may be indicative of unusual or potentially suspicious activity. These examples are not intended to be all inclusive; there may be other types of unusual behavior which could indicate a potentially suspicious activity. If an associate becomes aware of such activity, that person's manager, or the CCO, or his/her designee, should be notified using the Request for Compliance Review form.

Possible Red Flags and/or scenarios may include, but are not limited to:

1. Requesting a Free-Look within 30 days of the issuance of the contract.

2. Making a large overpayment of an initial premium and/or subsequent premium then requesting a refund from Athene.

3. Purchasing an insurance product that appears to be inconsistent with the customer's needs.

4. Submitting an unusual method of payment, particularly by cash or cash equivalents (when such method is, in fact, unusual) or payments from an OFAC/HM sanctioned or prohibited country

5. Purchasing an annuity with monetary instruments in structured amounts

6. Terminating an annuity early, especially at a cost to the customer, or where cash was tendered, and/or the refund check is directed to an apparently unrelated party. One example is canceling a contract that was received via Section 1035 exchange and requesting the money to be returned to a source other than the original company.

7. Exhibiting little or no concern for the investment performance of an insurance product, but much concern about the early termination features of a product.

8. Exhibiting reluctance to provide identifying information when purchasing an annuity, or the provision of minimal or seemingly fictitious information. An example would be a customer who exhibits unusual concern regarding the Company's compliance with government reporting requirements, particularly with respect to his or her identity, type of business and assets, or who is reluctant or refuses to reveal any information concerning business activities or furnishes unusual or suspect identification or business documents.

9. Making frequent or large premium deposits with no apparent business reason and without concern to the contract or tax consequences.

10. Purchasing a large contract or an account with unexplained or sudden extensive transfer activity in large amounts within the first 12 months.

11. Maintaining, for no apparent reason, multiple accounts under a single name or multiple names.

12. The customer has difficulty describing the nature of his or her business or lacks general knowledge of his or her industry.

13. The customer has been rejected or has had its relationship terminated as a customer by other financial services firms.

14. An account is opened by a politically exposed person (PEP), particularly in conjunction with one or more additional risk factors, such as the account being opened by a shell company beneficially owned or controlled by the PEP, the PEP is from a country which has been identified by FATF as having strategic AML regime deficiencies, or the PEP is from a country known to have a high level of corruption.

15. An account is opened by a non-profit organization that provides services in geographic locations known to be at higher risk for being an active terrorist threat.

16. An account is opened in the name of a legal entity that is involved in the activities of an association, organization or foundation whose aims are related to the claims or demands of a known terrorist entity.

17. Requesting that a transaction be processed in such a manner so as to avoid the Company's normal documentation requirements.

18. Exhibiting little or no concern for the performance of the contract but much concern for the early cancellation of the contract.

19. Attempting to use cash to complete a proposed transaction when this type of business transaction is normally handled by checks or other payment instruments.

20. Requesting to make a premium payment with foreign currency or with a wire transfer from a foreign country.

21. Exhibiting reluctance to provide normal information when applying for a contract, providing minimal or fictitious information or providing information that is difficult or expensive for the insurance company to verify.

22. Appearing to have contracts/accounts with several insurance companies.

23. Purchasing contracts in amounts considered beyond the customer's apparent means.

24. Applying for a contract where the source of the funds is unclear.

25. Frequently changing bank account details or information for disbursement proceeds, in particular when followed by redemption requests.

26. Outgoing checks to third parties coincide with, or are close in time to, incoming checks from other third parties.

27. Wiring monies to or from unrelated third parties (foreign or domestic), or where the name or account number of the beneficiary or remitter has not been supplied.

28. Transferring funds into an account and are subsequently transferred out of the account in the same or nearly the same amounts, especially when the origin and destination locations are high-risk jurisdictions.

29. There is an unusual use of trust funds in business transactions or other financial activity.

30. Law enforcement has issued subpoenas or freeze letters regarding a customer or contract.

31. Notifications received of potentially suspicious activity in customer contract. Such notifications can take the form of alerts or other concern regarding negative news, money movements or activity.

32. Wire transfer activity, when viewed over a period, reveals suspicious or unusual patterns which could include round dollar, repetitive transactions or circuitous money movements.

33. The customer engages in transactions that show the customer is acting on behalf of third parties with no apparent business or lawful purpose.

34. There is an unusual use of trust funds in business transactions or other financial activity.

35. To better assist the Company's associates in identifying AML Red Flags and what to do when they are discovered, we have created the AML Red Flags reference document which can be accessed on the Company's compliance website.

C) The following actions are strictly prohibited:

(1) Engaging in transfers of funds to or from OFAC/HM sanctioned countries or countries that have no apparent business purpose.

(2) Using wire transfers to move large amounts of money to an OFAC/HM sanctioned country or country that has no apparent business purpose.

7 Monitoring, Investigating, and Reporting

a) Monitoring

We will monitor through automated means where appropriate and practical, and through manual means where necessary and appropriate, for transactions identified in the previous sections. The CCO, or a designee, will review Exception Logs, Complaint Logs, Replacement Logs, and/or any other documentation that contains customer activity on a periodic basis to identify trends and patterns which could be indicative of money laundering. Any such trends or patterns discovered will be reported to the CCO or his/her designee who shall individually, or through delegation, investigate any such activity deemed to be suspicious and follow the reporting procedures set forth below as applicable.

b) Investigation

i) Whenever it is suspected that there may be a violation of the procedures set forth above or evidence of possible money laundering is discovered, the department supervisor or manager should be notified immediately. All information and documentation sufficient to make a meaningful assessment of the matter shall be assembled properly. Such information may consist of, but shall not be limited to, a copy of the complete contract owner and/or producer files, a listing of all parties involved, and a brief summary of the pertinent facts. Based upon the initial information collected, the department supervisor or manager shall make an initial assessment of the incident(s) and refer the matter to the CCO or his/her designee for further action. Referrals should be completed according to the process set out in the company's Anti-Fraud Plan.

ii) During the investigation, the CCO or his/her designee may consult with the Company's SIU and legal staff if appropriate. The CCO or his/her designee will comply with the Company's SIU procedures if appropriate and will comply with each state's laws regarding reporting and record-keeping requirements.

iii) During the course of an investigation, the Company will contact appropriate law enforcement when necessary, and especially in these emergencies:

(1) A legal or beneficial owner or person with whom the contract owner is engaged in a transaction is listed on or located in a country or region listed on the OFAC/HM lists;

(2) A contract owned by an entity (beneficial owner) or is controlled by a person or entity listed on the OFAC/HM lists;

(3) A customer tries to use bribery, coercion or similar means to purchase a contract or carry out a suspicious activity and we have reason to believe the customer is trying to move illicit cash out of the government's reach;

(4) We have reason to believe the customer is about to use funds to further an act of terrorism or other illegal activity; and

(5) In these emergency cases, Compliance will complete a Suspicious Activity Report and notify either OFAC, the US Attorney's Office in the jurisdiction where the transaction originates, the FBI, and/or other law enforcement officials as deemed necessary.

c) Reporting

i) Suspicious Activity Reports (SARs)

(1) All recommendations to file a SAR will be presented to the Legal and Compliance Vice President. The Legal and Compliance Vice President is responsible for informing the CCO of SARs filed. The Compliance Department will file form SAR for any transactions conducted or attempted through our company involving funds or cash value where we know, suspect, or have reason to suspect:

(a) The transaction involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity as part of a plan to violate or evade laws or regulations.

(b) The transaction is designed to evade the requirements of the Bank Secrecy Act or any similar law or regulation.

(c) The transaction has no business or apparent lawful purpose or is not the sort of transaction in which the customer would normally be expected to engage in, and we know after examining the transaction and other facts, that there is no possible purpose of the transaction and no reasonable explanation for the transaction.

(d) The transaction involves the use of the company to facilitate a criminal act or criminal activity.

(e) The transaction is not the type of activity normally expected for the type of product involved or used to conduct the transaction.

(2) We will not base our decision on whether to file a SAR solely on whether the transaction falls above a pre-set threshold ($5,000 +). We will file a SAR and notify appropriate law enforcement of all transactions that raise an identifiable suspicion of criminal, terrorist, or corrupt activities (even those less than $5,000).

(3) SARs may be reported to the Board of Directors and senior management at the discretion of the CCO; however, SARs will not be reported to anyone without the authorization of the CCO.

(4) We will report suspicious transactions and collect and maintain appropriate supporting materials as required. We will file a SAR no later than 30 days after the date of initial detection of a suspicious activity or transaction. If we cannot identify a suspect within 30 days, we may delay our filing of a SAR for an additional 30 days, but never for more than 60 days. *A separate SAR will be completed for each individual involved. One SAR is required when a sole producer and Athene are involved.

(5) We will keep copies of all SARs filed and the business record and supporting documentation for five years from the date of filing the SAR. We will identify and maintain supporting documentation and make such information available to FinCEN and other appropriate law enforcement agencies upon request.

(6) We will not notify any person involved in the suspicious activity or transaction that a SAR has been filed, except as permitted by law. Anyone who is subpoenaed or required to disclose SAR filing information, except where requested by FinCEN or other law agencies, will decline to produce the SAR or provide any information to disclose that a SAR was prepared or filed. We will notify FinCEN upon any such request.

8 Cooperating with Request for Information from Law Enforcement Agencies

a) We will respond to requests from FinCEN and other law enforcement agencies about contracts or transactions by searching our records to determine whether we maintain or have maintained a contract, or have engaged in any transaction with any individual, entity or organization named in such a request. The Compliance Department will be the point of contact for all such requests. We will conduct the search for activity for a period of 12 months prior to the date of the request, or for a period stated within the request. If we find a match, we will report it to the agency or individual who made the request. If we do not find a match, we will not reply, unless specifically instructed to do so in the request.

b) We will not disclose the fact that we have received a request for information, except as is necessary to comply with the request.

c) We will follow our Privacy Policy and procedures necessary to maintain security and privacy of information. All questions we have about a request will be directed to the requesting agency.

9 Sharing Information with Other Financial Institutions

a) We may share information about those suspected of money laundering with other financial institutions for the purposes of identifying and reporting activities that may involve money laundering activities and to determine whether to establish or maintain a contract or engage in a transaction. However, information will not be shared without the prior authorization of the CCO.

b) We will file an appropriate initial notice with FinCEN prior to sharing any information. Before we share with another financial institution, we will take reasonable steps to verify that the other institution has submitted a notice with FinCEN. This applies to affiliated companies as well as nonaffiliated companies. Only relevant information will be shared in accordance with our Privacy Policy.

10 Record Keeping

a) Records of information received or used in an investigation or while monitoring this Policy must be retained a minimum of five (5) years from the date the relationship has ended or longer if required by state or local law.

b) The Company must retain records of which documents were relied on, the results derived at, and records of how substantive discrepancies discovered while monitoring activity were resolved, for a minimum of five (5) years from the time the record was made.

11 Money Laundering Training Program

a) Home Office Staff

i) The CCO or his/her designee shall be responsible for providing Customer Service and New Business associates, as well as any other Company associates who have a reasonable expectation of dealing with or being exposed to money laundering acts on more than an occasional basis, with information and training relative to the detection of money laundering activities. We will provide Financial Crime Awareness Training to:

(1) New hires within the first 90 days (awareness training) and

(2) Existing employees every year.

Note: This training may be held in conjunction with or as part of other fraud related company training.

ii) Specific information relative to the requirements of the USA PATRIOT Act, the Company's AML Program, and how to identify "red flags" that could indicate suspicious behavior will be provided to all affected associates.

iii) The CCO or his/her designee shall maintain a record of each training session and a record of the attendees at such training.

iv) Failure of associates to complete such training will lead to disciplinary action, up to and including termination of employment.

b) Field Force

i) The CCO, or his/her designee, shall be responsible for determining and providing training on anti-money laundering to producers contracted by the company to sell and distribute its products. The CCO or his/her designee will determine the appropriate method and style of training to be provided, consistent with the standards set out by the U.S. Treasury. Training for the field force will occur initially before the issuance of the Company's product and every two years thereafter.

ii) The CCO or his/her designee may develop procedures for accepting certification of completion of training that producers may receive from other companies or sources.

iii) All new producers will certify to having received training on anti-money laundering or will be required to take such training as described below as part of the requirement to contract with the Company prior to the issuance of an annuity contract.

iv) Failure to take such training as required by the Company will lead to disciplinary action, up to and including termination of the producer's contract.

c) Training Program

i) The training provided to home office staff or to producers should cover, at a minimum, the following topics:

(1) Key Anti-Money Laundering Concepts

(2) Responsibilities of the Company and Individual

(3) Red Flags

(4) Know Your Customer Requirements

(5) Methods of Payment

(6) Suspicious Activity Monitoring and Reporting

(7) Record Keeping

(8) Penalties

12 Producer Integration

a) The Company uses contracted independent producers to market and sell its products. By the terms of the contract between the producer and the Company, producers agree to follow the Company's Policies and Procedures.

b) Producers have an important role to play in the Company's Anti-Money Laundering Program, since they have direct contact with customers and are thus often in the best position to gather information and detect suspicious activity. To assure that insurance companies and their distribution partners collaborate in preventing money laundering, the USA PATRIOT Act requires life insurance companies to integrate producers into their anti-money laundering programs and to monitor the producers' compliance with the programs. The Company will monitor producer compliance with the AML Program by ensuring training is completed.

c) While the Company and its producers collaborate in maintaining an effective anti-money laundering program, the Company is ultimately responsible for overseeing the program and for ensuring compliance with all laws, regulations, rules and internal policies and procedures.

d) Each producer should demonstrate behavior in the performance of his or her duties, under his or her contract with the Company, aligned with this Policy and the Anti-Money Laundering Program. Producers must understand that it is the policy of the Company to comply with all laws, regulations, and Company guidelines that apply to the business of the Company and to, wherever possible, prevent the occurrence of money laundering activities. Producers are expected to follow all policies and procedures with the understanding that not doing so may lead to disciplinary action, up to and including termination of their contract(s).

e) Regulations require the Company and producer to collaborate in the following areas:

i) Customer Information

(1) Collect the information required by the Company's Customer Identification Program, outlined in Section 5 above, from customers during the application processes. Producers must also certify that they have reviewed the information gathered and viewed it personally.

ii) Method of Payment

(1) Producers are authorized to accept only the initial premium on an insurance application. Producers are responsible to adhere to the Company's standards for acceptable forms of payment for initial and/or recurring premiums.

iii) Communication regarding Suspicious Transactions

(1) The Company is responsible for reporting suspicious transactions conducted through contracted producers. Regulations require the Company and producers to collaborate in identifying suspicious transactions that the Company must report. Accordingly, the Company's policies and procedures with respect to the reporting of suspicious transactions are listed below.

(a) Red Flags – Red flags that warrant consideration of a SAR are outlined in Section 6 above. Producers will be notified of the red flags that are most likely to come to their attention. Producers will be informed of how to communicate any suspicious activity to the CCO or his/her designee.

(i) New Business Red Flags - Producers may be in a key position to identify suspicious activity during the sales process. Producers will be notified that they should be alert for any red flags identified in Section 6 above. Producers will be informed of how to communicate any suspicious activity to the CCO or his/her designee.

(ii) In-force Red Flags - Following the issuance of a contract, producers should be alert for, and should report, any of the red flags identified in Section 6 above. Producers will be informed of how to communicate any suspicious activity to the CCO or his/her designee.

iv) Timing of Reports of Suspicious Activity - Producers will be notified that they are required to report suspicious activity to the CCO or his/her designee immediately, and/or to seek further guidance and instructions.

v) Follow-up and Reporting - When a producer detects any red flag, he or she may be requested to investigate further under the direction of the CCO or his/her designee or, in the case that the producer is affiliated with another broker/dealer, life insurance company, or bank, this direction may come from his or her own AML CCO. This may include gathering or attempting to verify additional information from the customer or from third-party sources.

(1) The Company's CCO or his /her designee will have sole responsibility for making a determination as to whether to file a SAR and whether a SAR should be filed jointly with other entities subject to federal anti-money laundering rules.

(2) The Company's CCO or his/her designee will be solely responsible for determining what information should be provided in response to requests for information concerning suspicious activity from customers, producers, and employees. Producers by law cannot notify any person involved in a transaction that the transaction has been reported.

vi) Confidentiality - SARs will be filed by the Company's CCO or his/her designee rather than the producer. The fact that a SAR has been filed or considered, and the contents of any SAR that has been filed, are strictly confidential. The CCO or his/her designee has the responsibility for responding to any inquiry regarding the subject matter of any SAR.

13 Independent Audit

a) The CCO is responsible for ensuring an independent audit is conducted to monitor and maintain an adequate AML Program. The Internal Audit Department shall maintain records of each independent audit it conducts and shall report the results of each audit to the CCO or his/her designee and to Senior Management. The CCO has the discretion to share independent audit findings with Internal Audit at his/her discretion. The CCO or his/her designee will address any resulting recommendations and findings.

b) The first audit of the Company's AML Program should occur no later than six (6) months after the effective date that the initial insurance industry regulations for the USA PATRIOT Act are adopted by the U.S. Treasury and independent testing to monitor and maintain an adequate program on a periodic basis thereafter.

14 Updating Policy and Procedures

The CCO or his/her designee shall be responsible for periodically assessing the Company's risks to money laundering activity, new or modified laws and regulations, new products, new distribution systems, and any other areas that may impact or require revision to this Policy. The CCO or his/her designee is responsible for overseeing any changes necessary and communicating those changes in an appropriate manner to all concerned parties, including home office associates, producers, senior management and regulators.

15 Other Related Policies and Procedures

a) Athene USA Privacy Policy
b) Athene USA Anti-Fraud Plan
c) Athene USA AML Policy and OFAC Adherence

Revision History

Change(s)	Change By	Approved By	Date
Updated references from Aviva to Athene and completed other changes recommended by Athene (clarified associated under 3b; 4a- CO is appointed by board or by direction of the board; 4c, CCO cannot delegate responsibility of CCO duties- only specific functions; 4d- interested parties; 5 is KYC not CIP; 6i clarified risk based approach & primary drivers; and 8b wires to any other account than the owner required compliance approval.	Mechile Adams	Dan Werner	07/20/2015
Removal of information about life insurance policies; minor working updates.	Mechile Adams	Dan Werner	12/4/2018
Updated staffing.	Mechile Adams	Lisa Arechavaleta	7/14/2019
Updated AML Program to include FINRA red flags published May 2019.	Mechile Adams	Lisa Arechavaleta	10/17/2019
General Updates	Brenda Branchcomb	Mechile Adams	11/13/2020
Annual review. General Updates.	Brenda Branchcomb	Mechile Adams	8/30/2021