GUGGENHEIM LIFE AND ANNUITY

Guggenheim Life and Annuity Company

Anti-Money Laundering Policy and Procedure

Sponsor
General Counsel

Owner
Senior Compliance Officer

Contact
Lisa.Harpenau@guggenhieminsurance.com

Effective Date
December 13, 2017

Table of Contents

1. Introduction

Guggenheim Life and Annuity Company, and its affiliates, Clear Spring Life Insurance Company and Paragon Life Insurance Company of Indiana, and any subsidiaries thereof (collectively, the "Company"), are strongly committed to preventing the use of its operations for money laundering or any activity which facilitates money laundering, or the funding of terrorist or criminal activities. This Policy and Procedure sets out the requirements and procedures associated with the anti-money laundering and anti-terrorism program ("AML").

1.1. Purpose

This Anti-Money Laundering Policy and Procedure (the "Company's AML Policy" or "this Policy") has been developed in compliance with the USA PATRIOT Act of 2001, which requires the Company to establish an AML program (the "AML Program") to include at a minimum:

- The development of internal policies, procedures and controls for AML;
- The designation of an AML Compliance Officer ("AMLCO") (see Appendix A – AML Compliance Officer (AMLCO) and Contacts);
- Requiring an ongoing training program for employees, independent contractors and independent agents; and
- An independent audit function to test the AML Program.

1.2. Scope

The Company's AML Policy applies to all transactions of the Company, including the Company's Customers, the issuance of and making of payments with respect to Covered Products and the due diligence of Counterparties. This Policy requires all employees, independent contractors and independent agents to:

- Read and acknowledge their understanding of the Company's AML Policy;
- Attend regular AML training programs if their position is designated by this Policy as requiring training;
- Avoid drawing conclusions about Customers and Counterparties and their activities based solely on the Customer's and Counterparty's religious affiliation, ethnicity or national origin; and
- Not inform Customers or Counterparties that their activities have been, may be or will be reported as suspicious or under investigation.

The Company's AML Policy is intended to supplement, but does not supersede, the Anti-Money Laundering Policy promulgated by Guggenheim Capital, LLC, and any amendments thereto.

2. Policy Statements

2.1. Policy Statement

The Company will comply with all applicable laws and regulations designed to combat money laundering activity and terrorist financing and will cooperate with the appropriate authorities in efforts to combat money laundering and terrorism by taking active measures to detect, monitor, report and prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities. Every employee, independent contractor and independent agent is required to act in furtherance of the Company's AML Policy to protect the Company from exploitation by money launderers or terrorists; employees, independent contractors and independent agents found violating this Policy will be subject to disciplinary action. In furtherance of this Policy, the Company designates herewith an AML Compliance Committee, consisting of the Company's general counsel, and certain compliance, finance, and accounting officers (see Appendix B – AML Compliance Committee) to periodically review and update this Policy and the Company's AML Program (as defined below).

3. Requirements

3.1. Responsibilities

3.1.1. Company Responsibilities.

As directed by this Policy, the Company will:

- Take reasonable steps to determine the true identity of all of the Company's Customers and Counterparties;
- Not knowingly accept funds from or conduct business with Customers and Counterparties whose money the Company believes is derived from criminal activity or is intended to conduct, finance or support terrorist or other illegal activities;
- Not ignore indications that a Customer's or Counterparty's money originated from criminal or other money laundering activities or is intended to conduct, finance or support terrorist or other illegal activities;
- Take appropriate measures, consistent with the law, when the Company becomes aware of red flags which lead to a reasonable suspicion of Customer or Counterparty activity;
- Cooperate fully with law enforcement and regulatory agencies to the extent that it can do so under all applicable foreign and domestic laws;
- Comply with Section 314(a) of the Patriot Act with respect to notices received from the Financial Crimes Enforcement Network of the U.S. Department of the Treasury ("FinCEN");

- Report all identified instances of suspicious activity to the extent that it can do so under all applicable laws;
- Comply with all anti-money laundering and anti-terrorism laws and regulations; and
- When suspicious activity is identified, file a Red Flag Escalation Form (See Exhibit A) with the AMLCO and, when determined appropriate by the AMLCO, in coordination with the Global AML Head, file a Suspicious Activity Report ("SAR") with FinCEN.

3.1.2. Statutory Prohibition against Disclosure.

As part of its obligations pursuant to federal law, the Company is required to file a SAR with FinCEN to report suspicious transactions relevant to a possible violation of law or regulation. There are statutory and regulatory prohibitions against the disclosure of information filed in, or the fact of filing, a SAR whether the report is required or is filed voluntarily. Thus, the Company, its employees, independent contractors and independent agents are specifically prohibited from disclosing that a SAR has been filed (or that the Company has received a copy of filed joint SAR from another financial institution involved in the same transaction) or the information contained therein, except to appropriate law enforcement and regulatory agencies.

If the Company is served with any subpoena requiring disclosure of the fact that a SAR has been filed, or of a copy of the SAR itself, except to the extent that the subpoena is submitted by an appropriate law enforcement or supervisory agency, the Company should neither confirm nor deny the existence of the SAR. The Company through its AMLCO may notify the Office of Chief Counsel at the Financial Crimes Enforcement Network (202) 728-8071 if such action is deemed warranted based on a review of the facts and circumstances. The Global AML Head shall also be informed.

The Company will not disclose to any party the fact that a 314(a) notice has been received, except to the extent allowable by law or as required to comply with the request. Disclosure of such information will be at the direction of the AMLCO and in accordance with the Company's procedures or existing agreements, ensuring such information is safeguarded and kept confidential.

Any Company employee, independent contractor or independent agent who violates any applicable anti-money laundering or anti-terrorism law or regulation, whether through intentional non-compliance, willful blindness or negligence, or fails to escalate red flags of potential suspicious activity about which they become aware, is subject to disciplinary action, such as probation, remedial training, adverse impact on promotions or compensation reviews, or termination. Also, if any Company employee, independent contractor or independent agent intentionally violates any applicable AML law or regulation, such action will be reported to regulatory and law enforcement officials in accordance with local laws and regulations.

3.1.3. Designation of AML Compliance Officer and AML Compliance Committee.

The person listed on Appendix A – AML Compliance Officer (AMLCO) and Contacts is the designated AMLCO with responsibility for the AML Program. The AMLCO is responsible for, among other things:

- Being thoroughly familiar with:
  - The operations of the Company's business;
  - All aspects of the AML Program;
  - The requirements of the Bank Secrecy Act;
  - Applicable FinCEN forms, including having read carefully all applicable documents issued or posted on FinCENs web page: www.fincen.gov;
- Developing a risk-based AML program;
- Monitoring of the Company's compliance with applicable anti-money laundering and anti-terrorism laws and regulations and with the AML Program;
- Being available to answer all questions posed by employees, independent contractors and independent agents;
- Updating the AML Program as needed and when necessary;
- Providing AML training and periodic retraining for employees, independent contractors, independent agents, brokers, and any others doing business with Covered Products;
- Designing AML training programs so that employees, independent contractors and independent agents have the knowledge necessary to comply with the AML Program;
- Reviewing all Red Flag Escalation Forms submitted by employees, independent contractors and independent agents and taking appropriate action; and
- Reviewing all 314(a) notices and positive matches.

Any questions regarding the Company's AML Policy or any suspicious questions or actions by Customers or Counterparties should be brought promptly to the attention of the AMLCO. Appendix B – AML Compliance Committee lists the designated members of the AML Compliance Committee.

3.1.4. Know Your Customer/Counterparty and Customer Identification Program – Overview.

Following Know Your Customer/Counterparty ("KYC") and Customer Identification Program ("CIP") policies and procedures decreases the chance that employees, independent contractors, independent agents or the Company will be used to facilitate money-laundering activities. In fact, knowing your Customer or Counterparty is the single most important deterrent to money laundering or other illegal conduct. It is unacceptable behavior to knowingly accept funds from or conduct business with Customers or Counterparties whose money the Company believes is derived from

criminal activity or is intended to conduct, finance or support terrorist or other illegal activities.

Customer and Counterparty identification is gathered through various processes, including new business, agent appointments, investments, vendor and other KYC/CIP processes.

The Company's KYC/CIP procedures include (at a minimum, and should be expanded where appropriate)[1]:

Customer

- Collecting identifying information about the Customer, including:
  - Full legal name;
  - Residential address (no P.O. boxes);
  - Social Security Number ("SSN") or Tax Identification Number ("TIN"); and
  - Date of birth.

- Having independent agents visually inspect and make copies of Customer driver's licenses or other Customer identification documents to verify the applicant's identity[2].
- Where the Customer is a trust or other entity, identifying the beneficial owner(s) and control person(s) of the Customer, where appropriate based on risk.

Counterparty

- Collecting and verifying, as appropriate, identification information about the Counterparty listed on the appropriate KYC Checklist attached to the Guggenheim Insurance Investment Policy and Procedure or as outlined in the Guggenheim Capital, LLC Vendor Risk Management Due Diligence Procedure:
- Collecting identifying information about the Customer, including:
  - KYC Checklist – Private Corporations & Transactions
  - KYC Checklist – Regulated Entities and Publicly Traded Companies
- Identifying the beneficial owner(s) and control person(s) of the Counterparty, where appropriate based on risk

3.1.5. Customer or Counterparty Profile.

The vast majority of Customers and Counterparties are not involved in money laundering, so it is important for the Company to be able to identify routine transactions versus suspicious transactions. Performing a needs analysis for a

[1] *Contact the AMLCO if you have questions whether expanded KYC/CIP is appropriate with respect to any Customer or Counterparty.*

[2] *An internet-based identification verification program (such as those available from LexisNexis or IDology, Inc.) will be used in place of physical identification to verify the identity of Customers acquiring Covered Products on a direct-to-consumer basis.*

Customer or Counterparty not only helps meet the KYC requirements but also benefits our business.

A complete profile for each Customer and Counterparty provides everyone the ability to:

- Verify the identity of the Customer or Counterparty;
- Verify the identity of all beneficial owners and control persons where appropriate;
- Ensure the financial information needed for KYC/CIP purposes is information normally collected in a needs analysis;
- Identifying high risk clients and assigning an AML risk rating for each Customer or Counterparty;
- Identify appropriate transactions and those that may need heightened scrutiny;
- Detect a pattern of activities that is inconsistent with the Customer's or Counterparty's stated goals and business;
- Detect inconsistent patterns of transactions; and
- Anticipate activities that may or may not be related to money laundering or conducting, financing or supporting terrorist activities and may require further investigation.

Customer and Counterparty identification is gathered through various processes, including new business, agent appointments, investments, vendor and other KYC/CIP processes , which, as applicable, are further outlined in the Guggenheim Insurance Investment Process and Procedure Policy or Guggenheim Capital, LLC Vendor Risk Management Due Diligence Procedure.

3.1.6. Enhanced Due Diligence.

A Customer's or Counterparty's location, affiliation or type of business may present a greater AML risk which would indicate a need for increased scrutiny. For example, regulators have identified PEPs (Politically Exposed Persons) as individuals that require greater due diligence. Additionally, other high risk parties, as set forth below, may also require enhanced due diligence to be conducted by the Company. If an employee, independent contractor or independent agent becomes aware that a third party requires enhanced due diligence per this section, the employee, independent contractor or independent agent must escalate the high-risk third party to the appropriate senior manager and the AMLCO for handling. The AMLCO will, as appropriate, escalate the matter to senior management. Enhanced due diligence might include more in-depth identification of owners and principals as well as searches of available litigation, public records, and/or press or media coverage. The AMLCO must obtain approval from the senior business unit manager and the Global AML Head and also consult with Guggenheim Capital's Chief Legal Officer prior to approving[3] a business relationship with any of the following high-risk third parties:

[3] *The Chief Legal Officer may, at his discretion, identify a high-risk third party or a type or group of third-parties that does not require*

- Current or former PEPs and, to the extent known and available, their immediate family and close associates;
- Individuals or entities, domestic or foreign, identified from screening (e.g., Thomson Reuter's World-Check) to be a confirmed match to a sanctioned party, country, or jurisdiction;[4]
- Foreign corporations and individuals (including an individual who is a beneficial owner or control person of an entity that may not be high risk),[5] that are residents of or nationals of High Risk Jurisdictions (*Link to List of High Risk Jurisdictions);*
- Individuals and entities, domestic or foreign, identified from screening, subject to Material Legal and Regulatory Actions;
- Foreign Banks and Correspondent Accounts;
- Non-operating Shell Companies; and
- Additional high-risk third parties include: (i) privately held armament manufacturers, dealers and intermediaries; (ii) privately held paper currency intensive businesses (e.g., money transfer agents, money brokers, casinos, check cashers, pawnbrokers); and (iii) privately held dealers in precious metals or jewels.

4. Administration

4.1. Periodic Review and Monitoring

4.1.1. Periodic Assessment.

The Company will establish procedures to periodically review its population of Customers and Counterparties in order to assess if any changes have occurred that would warrant enhanced due diligence or escalation of approval (i.e., a high risk party). The frequency and extent of this assessment should be based on any trigger event or periodically based on risk, and may involve obtaining or updating documentation. "Trigger event" may include changes to the Customer's or Counterparty's risk profile, changes in identification information such as ownership, the addition of a new account/relationship, any red flag, etc. This assessment will be in addition to any KYC/CIP performed on the Customer or Counterparty prior to entering into a contract or other agreement, as applicable. Any Customer or Counterparty deemed high risk shall be reassessed annually.

consultation to establish a business relationship. The Chief Legal Officer may, at his discretion, recommend that the approval to establish a business relationship with a high-risk third party be escalated to other senior managers in the business unit or entity, or to a governance committee of Guggenheim Capital, LLC.

[4] A "confirmed match" refers to a determination by the AMLCO that the Customer or Counterparty is the same person or is likely to be the same party designated by a sanctions authority, or is domiciled in a sanctioned country/jurisdiction, based on identifying information that may include but is not limited to a match against the DOB, address, or other information.

[5] While a high risk beneficial owner or control person of an otherwise non-high risk entity should generally result in the entity being classified as high risk, there may be circumstances that merit a lower risk rating. Such determinations should be discussed with the Global AML Head and a lower risk rating documented.

4.1.2. Independent Audit.

There will be a periodic independent audit to test and evaluate compliance with and the effectiveness of the AML Program. The internal audit department of the Company will perform this at least every two years.

4.1.3. Suspicious Activities.

Employees, independent contractors and independent agents are responsible for identifying the expected activities of Customers and Counterparties in order to establish a range of typical actions. Any fact or circumstance that falls outside this range of typical actions is termed a “red flag” by FinCEN and may be considered suspicious or unusual, especially where the economic gain is not obvious or clear.

If it is suspected or known that a transaction involves funds related to an illegal activity or is designed to avoid regulations, the relevant employee, independent contractor or independent agent must report the transaction to the AMLCO by completing the Red Flag Escalation Form (Exhibit A) and submitting the completed form to GLACCompliance@guggenheiminsurance.com. The AMLCO, upon review of the activity, shall escalate for discussion to the Global AML Head to determine if a SAR is merited. Only the AMLCO or an AML Compliance Committee member may file a formal SAR with FinCEN. For assistance with completing the Red Flag Escalation Form, please contact the Guggenheim Insurance Legal and Compliance Department or the AMLCO. Where the AMLCO in discussion with the Global AML Head determines that a SAR is not warranted, that decision rationale shall be carefully and completely documented.

Through performance of their daily activities, all employees, independent contractors and independent agents shall monitor Customer and Counterparty activity.

Although no single activity or factor is necessarily indicative of suspicious activity, all such instances of a single activity or factor that could be indicative of suspicious activity should be reported to the AMLCO.

The AMLCO will evaluate such single, potentially suspicious activity together with other factors, such as length of time the Company has known the Customer or Counterparty.

All employees, independent contractors and independent agents of the Company should frequently review and become familiar with the information contained in the attached Exhibit B – Suspicious Activity Guidance – “Red Flags”, which provides an extensive list of “red flag” events that may be indicators of suspicious activity.

(NOTE: The list printed in Exhibit B should not be considered comprehensive or all-inclusive. Each independent agent, independent contractors or employee must understand the intent of the law so that any suspicious activity – whether listed specifically herein or not – is detected and reported to the AMLCO.)

4.1.4. Record Retention.

Federal rules require that all records mandated under the anti-money laundering and anti-terrorism regulations:

- Be kept for five years; and
- In a reasonably accessible place and manner.

In addition, all documents related to the opening of accounts and verification of identity must be retained for five years after the account is closed and the termination of any policy or contractual agreement with the Customer or Counterparty. If a particular state insurance regulation requires certain documentation to be retained for a longer period, the records must be maintained for the longer time period. Any Customer or Counterparty identification information included in the Customer or Counterparty file, along with any information provided to the AMLCO, should be retained. Proper documentation of any actions taken in furtherance of the AML Program protects employees, independent contractors and independent agents from possible penalties.

4.2. Updates and Exceptions

4.2.1. Updates.

The Company shall review and update as appropriate the AML Program and this Policy as necessary, or at least annually, to maintain their effectiveness. Updates to the AML Program and this Policy shall be undertaken based on the recommendations of the AML Compliance Committee, the results of any testing and any changes in the Company's legal duties. In addition, as additional products are offered, the Company's AML Policy and associated red flags will be updated, as appropriate.

4.2.2. Modifications and Exception.

The AMLCO may make such modifications and exceptions to the policies and procedures implementing the AML Program as the AMLCO may deem reasonable and appropriate, provided that such modifications or exceptions are consistent with the Company's policy to maintain reasonable and effective policies and procedures to detect and deter money laundering, terrorist financing and transactions prohibited under any applicable anti-money laundering or anti-terrorism laws. Any such modifications or exceptions shall be documented in writing by the AMLCO.

4.3. Training

4.3.1. Employees and Independent Contractors.

All employees and independent contractors of the Company will be provided a copy of this Policy and will be required to read and acknowledge the policy. In addition to mandatory periodic review of this Policy, AML training will be provided to those employees and independent contractors whose job responsibilities include:

- Direct Customer or Counterparty contact;
- Access to view and/or execute Customer or Counterparty transactions;
- Processing payments to or from Customers or Counterparties;
- Negotiating investment transactions on behalf of the Company's general account or separate accounts; or
- Supervisory authority over any employee or independent contractor whose responsibilities are referenced in this section.

The AML training program will consist of a review of the Company's AML Policy and any additional programs and materials as the AML Compliance Committee may deem necessary or appropriate from time to time.

Training will take place (i) within 90 days of hiring of an employee or independent contractor, (ii) at the time of implementation of this Policy and (iii) at least once annually thereafter. All new hires will be provided a copy of the Company's AML Policy as a part of new employee and independent contractor orientation along with the required training. Documentation of employee and independent contractor training will be maintained by the Company's Legal and Compliance Department.

4.3.2. Independent Agents.

All independent agents will be required to complete AML training at the time of their initial appointment unless the agent provides evidence satisfactory to the AMLCO that equivalent training has been completed within two years prior to appointment. Required training will consist two parts. First, all independent agents will be required to read the Company's AML Policy and verify his or her knowledge of this Policy. Second, independent agents will be required to take Company-approved AML training, such as LIMRA, or provide a certificate of completion of an acceptable AML training session prior to issuance of new business. The Company's administrative system will maintain a record of the independent agent's compliance with this training program. If the independent agent is in default, no application provided through this independent agent will be processed until the independent agent fulfills the training requirement under this Policy.

4.4. Violations

4.4.1. Civil and Criminal Penalties.

The penalties associated with money laundering are severe. Fines may be up to $500,000 or twice the value of the property involved in the transaction, whichever is greater. .Property involved in the transaction may also be subject to seizure and forfeiture. Employees, independent contractors and independent agents of financial institutions can be fined individually and sentenced to up to 20 years of imprisonment for knowing or being willfully blind to the fact that the transaction involved illegal funds.

Employees, independent contractors and independent agents can protect themselves from charges of willful blindness by reporting any suspicious behavior to the AMLCO and retaining documentation of the report. In addition, any failure to comply with this Policy may result in disciplinary action against the employee or independent agent including but not limited to employment or, as applicable, appointment termination.

4.5. Supporting Procedures

4.5.1. Investigation of Red Flags for Possible Suspicious Activity Report Filing.

The AMLCO will perform the following procedures:

- Promptly review and investigate all Red Flag Escalation Form submissions;
- Escalate for review any red flags the AMLCO determines may warrant a SAR, or any red flags about which the AMLCO cannot resolve or determine to have a legitimate and credible explanation;
- If the AMLCO determines that the red flags escalation does not merit further review by the Global AML Head, the AMLCO shall clearly document his/her findings and basis for conclusion;
- If the AMLCO and the Global AML Head determine that further investigation is warranted, the AMLCO shall document that determination and take the necessary steps to promptly investigate;
- If the AMLCO and the Global AML Head determine that a SAR is warranted, the AMLCO shall file a report within 30 days of making that decision using FinCEN Form 101. The Global AML Head shall review Form 101 prior to filing.

4.5.2. Sanctions Compliance.

The Company must determine, in connection with the purchase of a policy, funding of an investment, or opening an account, or engaging a vendor whether the Customer's or Counterparty's (or its beneficial owner's and control persons) name appears on sanctions lists published by, or who may be the subject of sanctions administered or enforced by, the United States (including the US Department of Treasury Office of Foreign Assets Control and the US Department of State), the European Union, Her Majesty's Treasury-UK, the United Nations, or locally applicable sanctions regimes, or who is a resident of or domiciled in a Sanctions Country (collectively referred to as "Sanctions").

Upon receipt of an application or diligence materials, a Customer's or Counterparty's information must be recorded and checked to determine if a party, including the party's beneficial owner(s) or control person(s), is the subject of Sanctions. Names of Customers and Counterparties are checked prior to issuance and on a daily basis thereafter.

The Company will also run a Sanctions check on any person due to receive any distribution or benefit payment from an annuity (including any withdrawal, surrender, annuity payment or payment of a death benefit) before such distribution or benefit payment is made.

At the time of appointment, all individual agents and agencies are checked against World-Check to determine if they are listed on any Sanctions lists or otherwise present a direct or indirect Sanctions risk. A confirmation will also be made that the party is not resident of or domiciled in a Sanctions Country. Each Customer and Counterparty will also undergo the same process.

The company may not do business with and prohibits any dealings, either directly or indirectly, with sanctioned parties or sanctioned countries/jurisdictions. This includes transactions in any security or financial instrument that may be subject to sanctions. Doing business with a person or entity that is sanctions may result in a civil fine and/or criminal penalties. For more information and requirements, please refer to the Guggenheim Capital, LLC Sanctions & Anti-boycott Policy.

The following steps are taken with regard to information obtained from World-Check or where a Sanctions risk has been identified:

No Matches: The Company will retain copies of all search results of names against updated World-Check lists.

False Positives or Possible Matches: In the event that a search result yields an AML-related “hit” or exception, the AMLCO will request additional identifying information from the affected person. The AMLCO will review the additional documentation to determine whether the “hit” is a false positive or a possible World-Check match. Note that World-Check may result in a hit that is not AML-related, such as a FINRA action. Where such action is considered to present material negative information (e.g., involves false statements, fraud, corruption or other) escalation to the Global AML Head is required.

Where the AMLCO determines that the hit is a false positive or not material, the AMLCO will create a memo to the file which includes the World-Check exception report, indicating that the “hit” is an AML-related false positive, but not a match, and will retain the supporting documentation with the exception.

If the identifying information provided by the affected person is insufficient to resolve the AML-related “hit” or exception, the AMLCO will make a determination whether to conduct enhanced due diligence in an effort to resolve the exception and to escalate to the Global AML Head. The AMLCO will file and retain the exception report, resolution (e.g., false positive), and the copies of the supporting documentation.

4.5.3. Customer Payments.

In furtherance of this Policy, the Company is prohibited from accepting certain forms of payment as outlined in the Guggenheim Insurance Check Acceptance Policy. Specifically, the Company is prohibited from:

- Accepting cash (coin or currency), money orders or travelers checks for any transaction;
- Accepting negotiable checks drawn on independent agent accounts;
- Accepting foreign checks; or
- Accepting personal checks drawn on anyone other than the contract owner with the exception of checks drawn on the account of legal guardian of a minor, parent or grandparent of a minor.

4.5.4. Information Sharing with Law Enforcement and Supervisory Authorities.

The following policies and procedures apply to all transactions involving the Company, not just those involving Covered Products.

A regulatory or law enforcement agency or supervisory authority investigating terrorist activity or money laundering, corruption or other misconduct may request information from the Company to facilitate an investigation. Any request from a law enforcement or regulatory authority, including any 314(a) notice, shall be escalated to the AMLCO who will determine if informing the Global AML Head and the Guggenheim Insurance Chief Counsel is warranted for further review and response. The Company shall cooperate with lawful requests for information from such authorities. If any employee, independent contractor or independent agent receives such a request, he or she must promptly alert the AMLCO.

The AMLCO is the point of contact for the Company for investigative issues or similar requests for information from law enforcement or supervisory authorities. All such requests must be referred to the AMLCO.

5. Reference

5.1. Definitions

Term	Definition
Beneficial Owner	A Beneficial Owner is any individual who owns 25% or more of the equity interest of a third party or the beneficial owner of an annuity contract such as a trust.
Control Person	A Control Person, who may or may not also be a beneficial owner, is to any person with significant control or management over a

	Party (e.g., an executive officer, senior management or any other individual who regularly performs similar functions).
Correspondent Account	An account maintained by a domestic financial institution on behalf of a foreign financial institution to receive deposits from, or make payments on behalf of a foreign financial institution, or to handle transactions related to sch an institution, and requires a formal relationship through which the financial insitution provides regular service. Foreign Financial Institution includes a foreign bank, foreign branch of the domestic bank, broker dealer in securities, future commission merchant, introducing broker or mutual fund, currency dealer or exchanger or a money transmitter.
Counterparty	Counterparty includes issuers, borrowers, all directors, senior officers and control persons of an issuer or borrower, and any other third party including vendors.
Covered Products	Covered products include investments, life insurance policies and annuity contracts which are (1) individual annuities, (2) fixed, indexed or variable, and (3) immediate or deferred.
Customer	Customers include applicants, contract owners, annuitants, beneficial owners/control persons, beneficiaries (including trusts) and independent agents contracted with the Company.
Cyber Security Event	Refers to any act or attempt, whether successful or not, to gain unauthorized access to disrupt, or misuse a firm's electronic systems or information stored on such systems. Where such act or attempt is intended to affect a transaction conducted or attempted by, at or through a firm, or to impact the critical systems of a firm, a suspicious activity report may be required.
Foreign Bank	Refers to a foreign bank operating under any one or more of the following: An offshore banking license. The USA PATRIOT Act (31 USC 5318(i)(4)(A) and 31 CFR 1010.605(i)) defines an offshore banking license as a license to conduct banking activities that, as a condition of the license, prohibits the licensed entity from conducting banking activities with the citizens, or in the local currency of, the jurisdiction that issued the license. A banking license issued by a foreign country (outside of the jurisdiction in which the relationship is being established) that has been designated as non-cooperative with international AML principles or procedures by an intergovernmental group or organization of which the United States is a member, and with which designation the United States representative to the group or organization concurs. The Financial Acction Task Force

	(FATF) is the only intergovernmental organization of which the United States is a member that has designated countires as non-cooperative with international anti-money laundering principles. The United States has concurred with all FATF designations to date. A banking license issued by a foreign country that has been designated by the US Secretary of the Treasury as warranting special measures due to money laundering concerns.
Foreign Shell Bank	A Foreign Shell Bank is an offshore bank without a physical presence in any country. Dealing with a Foreign Shell Bank is prohibited.
High Risk Jurisdictions	The List of High Risk Jurisdictions includes: (i) countries subject to Sanctions, including state sponsors of terrorism, human rights violators, disruptors of democratic processes, (ii) jurisdictions determined to be of money laundering concern by the U.S. Department of Treasury, and/or the Basel AML Working Group; (iii) jurisdictions or countries identified as non-cooperative by the Financial Action Task Force on Money Laundering; (iv) "Other Countries/territories of Concern" as defined herein; and (v) countries ranked 55 or above in the Transparency International Corruption Perceptions Index.
Integration	Integration is the third stage of money laundering where the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses.
Layering	Layering is the second stage of money laundering where funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin.
LIMRA	LIMRA International is a worldwide association providing research, consulting, and other services to nearly 850 insurance and financial services companies in more than 60 countries. LIMRA was established in 1916 to help its member companies maximize their marketing effectiveness.
Material Legal and Regulatory Actions	Include: (i) a felony criminal conviction; (ii) an expulsion or current suspension from membership or participation in a self-regulatory organization (e.g., FINRA, MSRB[6]) or the foreign equivalent of a self-regulatory organization, or a domestic or foreign securities or futures exchange; (iii) a bar or current suspension imposed by the Securities and Exchange Commission ("SEC") or other self-regulatory organization or foreign financial regulatory authority;

[6] Municipal Securities Rulemaking Board

	(iv) a denial or revocation of registration by the SEC, the Commodity Futures Trading Commission, or a foreign financial regulatory authority; (v) a finding that a member or person associated with a member has made false statements in applications or reports made to, or in proceedings before, a self-regulatory organization; or (vi) any regulatory action by a state insurance department, state securities department, or a state's attorney general office for engaging in dishonest or fraudulent practices.
Money Laundering	Money Laundering is engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the unlawful proceeds appear to have derived from legitimate origins or constitute legitimate assets. Generally, money laundering occurs in three stages: Placement, Layering and Integration.
Other Countries or Territories of Concern	Countries or Territories which are not Sanctioned Countries but which present potential reputational risk due to sanctions against certain goverment actors or organizations (e.g., sanctioned parties invovled in forced recruitment of child solders in the Central Africa Republic). These countries generally include: Belarus, Burundi, Central Afraica Republic, Democratics Republic of Congo, Eritrea, Ivory Coast, Lebanon, Libya, Myanmar, Palestinian Authorities, Russia, Somalia, Sudan, Venezuela, Yemen and Zimbabwe.
Sanctioned Country	Any country or region subject to broad restrictions due to its: sponsorship of terrorism, human rights abuses, or undermining democratic processes. Current Sanctioned Countries under this Policy include: Crimea region, Cuba, Iran, North Korea and Syria.
Sanctioned Party	Refers to any person or entity who is: (i) listed on a sanctions list published by the United States, European Union, Her Majesty's Treasury-UK, United Nations or locally applicable sanctions regime; (ii) the subject or target of sanctions, even if not specifically listed on a sanctions list; or (iii) a resident of or domiciled in the Crimea region, Cuba, Iran, North Korea, or Syria.
Shell Companies	Refers to non-publicly traded coroprations, limited liablity companies (LLCs), and trusts that typically have no physical presence (other than mailing address) and generate little to non independent economic value.
PEP/ Senior Foreign Political Official	PEP (Politically Exposed Person) is defined as (1) a "senior foreign political figure" who is a senior official in the executive, legislative, administrative, military or judicial branches of a foreign government (whether elected or not), a senior official of a major foreign political party, or a senior executive of a foreign government-owned corporation (It is important to note that while

	government-owned corporations may present risks of their own, the government-owned corporations themselves are not within the definition of a "senior foreign political figure." A senior political figure includes any corporation, business, or other entity that has been formed by, or for the benefit of, a senior foreign political figure.); (2) immediate familyof a political figure including parents, siblings, spouse, children, and in-laws; (3) a close associate of a senior political figure who is widely and publicly known to maintain an unusually close relationship with the senior foreign political figure, including a person who is in a position to conduct substantial domestic and international financial transactions on behalf of the senior foreign political figure. In some jurisdictions outside the United States, a "PEP" could also be considered "domestic" and therefore potential risks may need to be assessed of such "domestic PEP."
Placement	Placement is the first stage of money laundering where cash first enters the financial system. Cash generated from criminal activities is converted into monetary instruments, such as money orders or traveler's checks or deposited into accounts at financial institutions.
Suspicious Activity Report (SAR)	A Suspicious Activity Report or SAR is a report filed by the Company with FinCEN pursuant to federal law which requires the reporting of suspicious transactions.

Appendix A – Anti-Money Laundering Compliance Officer (“AMLCO”) and Contacts

PRIMARY CONTACT and AMLCO

Ryan T. Cloud
General Counsel
312 357 0531

SECONDARY CONTACTS

Stephen M. Coons
Chief Legal Officer
317 574 2661

Kimberly Davis
Senior Vice President and Assistant Treasurer
317 574 2056

Lisa Harpenau
Senior Compliance Officer
317 574 2068

Appendix B – Anti-Money Laundering Compliance Committee Members

Ryan T. Cloud
General Counsel

Stephen M. Coons
Chief Legal Officer

Kimberly Davis
Senior Vice President

Ellyn M. Nettleton
Senior Vice President, Controller and Treasurer

Joseph Bentivoglio
Senior Vice President, Administration

Judith Eppich
Vice President, Policy Service/Claims

Lisa Harpenau
Senior Compliance Officer

Exhibit A – Red Flag Escalation Form[7]

GUGGENHEIM LIFE AND ANNUITY

GUGGENHEIM LIFE AND ANNUITY COMPANY
401 PENNSYLVANIA PARKWAY, SUITE 300
INDIANAPOLIS, INDIANA 46280
GUGGENHEIMLIFE.COM

Internal Company Form
AML-RFE-0917

Red Flag Escalation Form
(Anti-Money Laundering Program "AML")
*Items marked with * are required.*
Please provide as much information as available regarding the red flag activities that prompted this report.

Date of report*: _____
Is this an amendment to an existing report? ❑ Yes ❑ No If yes, date of original report: _____

PART I. SUBMITTER'S INFORMATION

1. First and last name*: _____
2. Relationship of Submitter to Company (select one)*:
   ❑ Employee. Position:
   ❑ Independent Agent.
   ❑ Other: _____
3. Street address of office(s) where activity occurred*: _____
4. City, State, Zip*: _____
5. Country, if not U.S.: _____
6. Work phone number*: _____

PART II. SUBJECT'S INFORMATION

7. Subject is an*: ❑ Individual ❑ Entity
8. Check if: ❑ Multiple Subjects ❑ Subject's information unavailable
9. Entity name: _____
10. Type of business: _____
11. Subject first name: _____
12. Subject last name: _____
13. FEIN/TIN/SSN # (no dashes): _____
14. DOB (if applicable): _____
15. Street address: _____
16. City, State, Zip: _____
17. Subject's phone number: _____

AML-RFE-0917 | 06/2017 GLACCompliance@GUGGENHEIMINSURANCE.COM | Page 1 of 5

[7] *The existence of a "red flag" does not necessarily mean such "red flag" is evidence of suspicious activity or that a SAR is required. Red flags simply require that a review/investigation be conducted.*

GUGGENHEIM LIFE AND ANNUITY

GUGGENHEIM LIFE AND ANNUITY COMPANY
401 PENNSYLVANIA PARKWAY, SUITE 300
INDIANAPOLIS, INDIANA 46280
GUGGENHEIMLIFE.COM

PART II (CONTINUED)

18. Country, if not U.S.: _____
19. Subject's role in reported activity: _____
20. Government issued identification (if available): _____
21. ID Number: _____
22. Issuing state or country: _____

PART III RED FLAG ACTIVITY INFORMATION

23. Amount involved in this report:
$_____
❑ Amount Unknown
❑ No Amount Involved

25. Date range of red flag activity:
From: _____
To: _____

26. Policy/Contract number(s) in connection with red flag activity (list the contracts and indicate whether they are closed/terminated):

27. Money laundering flag (Check all that apply):
❑ Source of funds
❑ Designation of beneficiaries, assignees, or joint owners
❑ EFT/wire transfers
❑ Receipt of government payment/ benefits
❑ Transaction out of pattern for customer
❑ Use of multiple accounts
❑ Use of noncash monetary instruments
❑ Use of third-party transactors (straw man)
❑ Early surrender/withdrawal
❑ Other:_____

28. Covered product type (Check all that apply):
❑ Annuity contract
❑ Permanent life insurance policy
❑ Other (explain in Part IV)

29. Type of red flag activity:
❑ Money laundering
❑ Terrorist financing
❑ Other (explain in Part IV)

30. Structuring (Check all that apply):
❑ Alters transaction to avoid BSA recordkeeping requirement
❑ Multiple transactions below BSA recordkeeping threshold
❑ Inquiry by customer re BSA recordkeeping requirements
❑ Alters transactions to avoid CTR requirement
❑ Other: _____

31. Identification documentation (Check all that apply):
❑ Changes spelling or arrangement of name
❑ Multiple individuals with same or similar identities
❑ Provided questionable or false documentation
❑ Refused or avoided request for documentation
❑ Single individual with multiple identities
❑ Other: _____

GUGGENHEIM LIFE AND ANNUITY

GUGGENHEIM LIFE AND ANNUITY COMPANY
401 PENNSYLVANIA PARKWAY, SUITE 300
INDIANAPOLIS, INDIANA 46280
GUGGENHEIMLIFE.COM

PART III (CONTINUED):

32. Other red flag activities:
- ❑ Account takeover
- ❑ Bribery or gratuity
- ❑ Counterfeit instruments
- ❑ Elder financial exploitation
- ❑ Excessive insurance
- ❑ Excessive or unusual cash borrowing against policy/annuity
- ❑ Forgeries
- ❑ Identity theft
- ❑ Little or no concern for product performance, tax or surrender charges
- ❑ Misuse of "free look" period
- ❑ Misuse of position or self-dealing
- ❑ Proceeds sent to or received from third party
- ❑ Unclear or no insurable interest
- ❑ Unlicensed or unregistered money services business
- ❑ Suspected public/private corruption (domestic)
- ❑ Suspected public/private corruption (foreign)
- ❑ Life settlement sales insurance (i.e. viaticals)
- ❑ Termination of policy or contract
- ❑ Use of informal value transfer system
- ❑ Use of multiple transaction locations
- ❑ Transaction with no apparent economic, business or lawful purpose
- ❑ Two or more individuals working together
- ❑ Unauthorized electronic intrusion
- ❑ Other: _____

PART IV RED FLAG ATIVITY INFORMATION – NARRATIVE

Explanation/Description of red flag activity(ies): The completion of this section is **critical**. The care with which it is completed may determine whether or not the described activity and its possible criminal nature are clearly understood by the Company's AML Compliance Officer. Provide a clear, complete and chronological narrative description of the activity. The narrative should address as much of the information listed in the checklist as possible. **Information already provided in earlier parts of this form need not be repeated if the meaning is clear. Attach additional pages and documentation as necessary.**
❑ Check here if additional materials are being provided.

A. Describe the conduct that raised red flags.

B. Explain whether the transaction(s) was completed or only attempted.

C. Describe the supporting documentation.

GUGGENHEIM LIFE AND ANNUITY

GUGGENHEIM LIFE AND ANNUITY COMPANY
401 PENNSYLVANIA PARKWAY, SUITE 300
INDIANAPOLIS, INDIANA 46280
GUGGENHEIMLIFE.COM

PART IV (CONTINUED)

D. Explain who benefited, financially or otherwise, from the transaction(s), how much and how (if known).

E. Detail the relationship (or lack thereof) between the insured/annuitant, policy/contract owner, beneficiary & person/entity paying premiums.

F. Indicate any frequent or unusual changes in the policy/contract.

G. Specify an unexplained death or payment to a beneficiary in a foreign jurisdiction.

H. Indicate whether U.S. or foreign currency and/or U.S. or foreign negotiable instrument(s) were involved. If foreign, provide the amount, name of currency and country of origin.

I. Indicate any wire transfers in or out and identifier numbers, including the transfer company's name.

PART V. RED FLAG REPORT CERTIFICATION

By signing this Red Flag Escalation Report, I certify that the information contained herein is truthful and accurate to the best of my knowledge*.

Signature _____ Date _____

GUGGENHEIM LIFE AND ANNUITY

GUGGENHEIM LIFE AND ANNUITY COMPANY
401 PENNSYLVANIA PARKWAY, SUITE 300
INDIANAPOLIS, INDIANA 46280
GUGGENHEIMLIFE.COM

- FOR AML COMPLIANCE OFFICER USE ONLY –

Date Report Received: _____

Notes:

Conclusion of findings:
- ❑ Activity as described would not constitute a violation of policy: No action necessary or taken.
- ❑ Report has been investigated and no violation of policy has occurred: No action necessary or taken.
- ❑ Report has been investigated and **will be escalated to senior management per proper procedure.**

Signature of AML Compliance Officer:

_____
Signature

_____
Date

Exhibit B – Suspicious Activities Guidance – “Red Flags”

New Business Customer Red Flags

Red flags to watch for during transactions involving the sale and issuance of new business include the following:

- The Customer buys an insurance product that appears to be inconsistent with his or her needs.
- The source of the funds used to purchase the product is inconsistent with the Customer’s financial situation or profile.
- The Customer exhibits unusual concern with government reporting requirements, especially those requiring personal identification information.
- The Customer wishes to engage in a transaction that lacks business sense or apparent investment strategy or is inconsistent with the Customer’s stated business strategy.
- The Customer appears to be acting as an agent for an undisclosed party or principal but is reluctant or refuses to provide information about that party.
- The Customer (or a person associated with the Customer) has a questionable background or is the subject of news reports indicating possible criminal, civil or regulatory violations.
- The Customer provides inconsistent answers to questions or misleading information.
- The Customer lives in a distant locale, though a comparable policy could be purchased where he or she lives.
- The Customer shows little or no concern for the investment performance of an insurance product but much concern about its withdrawals and surrender provisions.
- The Customer exhibits a lack of concern for policy fees and charges, especially early surrender charges.
- The Customer is reluctant to provide identifying information when purchasing an insurance product.
- The Customer provides minimal or seemingly fictitious information.
- The Customer exercises the “free-look” privilege shortly after the policy is issued.

Premium and Deposit Red Flags

Red flags associated with premium and deposit payments include the following:

- Any unusual method of payment, particularly by cash or cash equivalents.
- Payments received from unrelated third parties.
- Payments that are made through wire transfers of sizable amounts.
- The purchase of an insurance product with monetary instruments in structured amounts (“structured settlements”).

- The purchase of an insurance policy with numerous checks drawn on different accounts.
- Large payments that are followed closely by requests for partial surrenders or withdrawals.

Policy / OTHER Activity Red Flags

Many policy transactions are a normal part of insurance transactions and insurance business. Red flag activities are any that are unusual or atypical. Examples include the following:

- The early termination of an insurance product, especially at a cost to the Customer or where cash was tendered and/or the refund check is directed to an apparently unrelated third party.
- Lack of Customer concern or questions about surrender charges when requesting a policy surrender.
- The transfer of policy ownership to an apparently unrelated third party.
- Withdrawing a significant portion of the account value of the contract soon after its purchase.
- Payment of unscheduled premiums, followed shortly by one or more policy withdrawals.
- Any request that a transaction be processed in a manner such as to avoid normal documentation or normal procedures.
- Activity, or attempted activity, involving a Cyber Security Event;[8]

All employees should also be aware of the requirement to escalate a cybersecurity event to the Information Security team who will coordinate with the Global Head of AML, as appropriate.

A Cyber Security event refers to: *any act or attempt, whether successful or not, to gain unauthorized access to disrupt or misuse a firm's electronic systems or information stored on such systems*.

Where such act or attempt is intended to affect a transaction conducted or attempted by, at or through a firm, or to impact the critical systems of a firm, a SAR may be required.

The Information Security team: InformationSecurity@GuggenheimPartners.com

Independent Agent and Employee Red Flags

Not all red flags arise from the Customer's side of the transaction. Some are raised by suspicious activity demonstrated by the independent agent or a Company employee. Usually these red flags relate to a change in the independent agent's sales activity or employee's behavior. The change may be observed by the independent agent's or employee's manager, a field compliance principal or a compliance officer. However detected, the matter is escalated to the AMLCO or AML Compliance Committee. There may well be valid reasons for observed changes, but those would be determined only after a compliance review.

The following examples illustrate activity that suggests a need for closer review [9]:

> *Agent Sarah has been an average producer in the agency for the three years she has been associated with it. This year, she suddenly (and unexpectedly) exhibited a dramatic increase in*

[8] *"Cyber Security Event" is defined in Section 5.1.*

[9] *From "Anti-Money Laundering for the Insurance Industry", ©2008 by WebCE, Inc. Reprinted with permission.*

sales, especially with limited premium permanent life insurance policies. Many of those policies have experienced frequent loans and withdrawals.

Employee Bill has always had a modestly comfortable lifestyle. In the past several months, he has been spending money like there's no tomorrow, from major home improvements and a new sports car to dining out frequently and taking expensive vacations.

Producer Daryl experiences consistently high activity in single premium contracts that exceed company averages.

Agent Steve anxiously asks a compliance department employee what she may know about a case being reviewed by the company's AML compliance committee. (Note: For privacy reasons, most financial services companies prohibit producers from obtaining personal customer information at the company level.)

Broker Karen writes a high number of policies for customers who live away from her normal business market, although many are returned during the free-look period.