Anti-Money Laundering Program

Policy

It is the policy of Palomar Holdings, Inc., Palomar Excess and Surplus Insurance Company, Palomar Specialty Insurance Company, and all affiliates (for the purposes of this Policy, collectively, "Palomar" or "Company") to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities by complying with the Bank Secrecy Act ("BSA") and its implementing regulations.

Regulators have deemed money laundering to include any of the following types of activities:

- Engaging in financial transactions involving funds derived from criminal activities.
- Engaging in financial transactions in furtherance of criminal activity.
- Engaging in any activity designed to prevent detection of the fact that the funds were derived from criminal activity.
- Structuring, or participating in structuring, of transactions to evade money laundering reporting requirements.

Purpose/Scope

Palomar's Anti-money Laundering ("AML") Program is designed to ensure compliance with all applicable BSA regulations and other related SEC, Self-Regulatory Organization and Treasury regulations, and where applicable, relevant rules of the bank regulatory agencies. The program will be reviewed and updated on a regular basis to ensure appropriate policies, procedures and internal controls are in place to account for both changes in regulations and changes in our business.

The AML Program for Palomar is also the AML Program for its insurance subsidiaries and affiliates. Hereafter, when the term Palomar is used, it is inclusive of Palomar Excess and Surplus Insurance Company and Palomar Specialty Insurance Company.

The AML Program is also designed to ensure compliance with the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA Patriot Act) including Section 352 which requires the program to include the following elements:

- Development of internal policies and procedures.
- Appointment of an AML Compliance Officer.
- Ongoing training.
- Implementation of an Independent Audit function to test AML Program

Palomar's AML Program is based on an assessment of risk associated with Palomar's customers, structure, size, products and services, sales force, distribution channels, cash processing practices, and other relevant factors. Risks are periodically reassessed, and the AML Program is updated if necessary.

The Importance of an AML Program for Palomar

Federal law prohibits financial institutions from knowingly engaging in, or assisting with, money laundering activities. This concept of 'knowledge' is extremely broad, and a financial institution can be guilty of money laundering if it intentionally ignores certain suspicious activities. In addition to detecting and deterring money laundering activities, financial institutions also have a duty to report suspicious activities to the federal government.

Financial institutions and their associates are vulnerable to attempts by criminals to launder money. If such activities occur and Palomar determines that the Company or its associates knowingly participated in such activities, Palomar and/or the associate may be guilty of money laundering.

Although money laundering is usually associated with cash, it is not a required component in a transaction. Any financial transaction may be part of a process to obscure the origin of illegal funds. Day-to-day activities of Palomar associates can, theoretically, be part of a money laundering scheme including opening an account, processing checks, executing buy/sell orders, and processing transactions such as wire transfers and check withdrawals.

Therefore, Palomar associates need to understand what money laundering is, their role in identifying and combating it, and how to apply the policies and procedures of Palomar's AML Program to their jobs. Failure to comply could result in significant criminal, civil, and disciplinary penalties including:

- Fines up to twice the amount of the transaction up to $1 million.
- Employees of financial institutions can be fined individually and sentenced to up to 20 year of imprisonment for knowing or being willfully blind to the fact the transaction involved illegal funds.

Covered and Excluded Products

Products included in the Palomar AML Program (covered products) are:

- Insurance products with cash value and investment features.

Products excluded from the Palomar AML Program are:

- Property and Casualty
- Earthquake
- Wind
- Inland Marine
- Cyber
- Flood
- Reinsurance contracts

Palomar

Accountability

The Corporate Compliance Officer and Chief Privacy Officer for Palomar is the company's designated AML Compliance Officer. The AML Officer has working knowledge of the BSA and its implementing regulations and is qualified by experience, knowledge, and training; and has full responsibility and authority to enforce Palomar's AML Program.

The AML Officer may delegate some of the duties of the AML Compliance Officer to the Anti-Fraud and Financial Crimes Leader, or other qualified designee, but the Officer is responsible for overseeing the day-to-day AML Compliance Program.

The Palomar AML Compliance Officer shall:

- Monitor Palomar's compliance with AML obligations.
- Oversee the implementation of new AML requirements or changes to existing AML requirements.
- Ensure that appropriate Suspicious Activity Reports (SARs) are filed with FinCEN whenappropriate.
- Ensure all required AML records are maintained.
- Provide periodic updates to the Chief Legal Officer regarding the AML Program.
- Oversee the delivery of AML communications and training to associates.
- Interact with designated AML Compliance Officers of subsidiaries.

Information Sharing with Government Agencies and Other Financial Institutions

Financial Institutions

Section 314 of the USA Patriot Act is intended to facilitate the sharing of information between governmental entities and financial institutions (314(a)) and between financial institutions themselves (314(b)). The purpose of this sharing is to identify, prevent, and deter money laundering, and terrorist activity.

The USA Patriot Act provides that sharing information with government agencies and other financial institutions under 314(a) and (b) "shall not constitute a violation" of the privacy provisions of the Gramm-Leach-Bliley Act.

Information Sharing with Government Agencies – Section 314(a)

Palomar will respond to a Financial Crimes Enforcement Network (FinCEN) request concerning accounts and transactions (314(a) Request) by searching its records to determine whether it maintains orhas maintained any account for, or has engaged in any transaction with, each individual, entity or organization named in the 314(a) Request as outlined in the Frequently Asked Questions (FAQ) located on FinCEN's secure website. Unless otherwise stated in the 314(a) Request or specified by FinCEN, Palomar will search those documents outlined in FinCEN's FAQ. If Palomar finds a match, it will be reported to FinCEN via FinCEN's web-based 314(a) Secure Information Sharing System within 14 days or within the time requested by FinCEN in the request. If

the search parameters differ from those mentioned above (e.g., if FinCEN limits the search to a geographic location), Palomarwill structure the search accordingly.

If Palomar searches its records and does not find a matching account or transaction, then it willnot reply to the 314(a) Request. Palomar will maintain documentation that the required searchhas been performed. Such documentation will be maintained in the Sanctions Screening software system which will maintain a log of the number of accounts searched and whether a match was found.

Palomar will not disclose the fact that FinCEN has requested or obtained information, except tothe extent necessary to comply with the information request. Palomar will review, maintain, and implement procedures to protect the security and confidentiality of requests from FinCEN similar to those procedures established to satisfy the requirements of the Gramm-Leach-Bliley Act with regard to the protection of customers' nonpublic information.

Palomar will direct any questions regarding the 314(a) Request to the requesting federal law enforcement agency as designated in the request.

Unless otherwise stated in the 314(a) Request, Palomar will not be required to treat the information request as continuing in nature and will not be required to treat the periodic 314(a) Requestsas a government-provided list of suspected terrorists for purposes of the customer identification and verification requirements.

Voluntary Information Sharing with Other Financial Institutions – Section 314(b)

Palomar may share information regarding individuals, entities, organizations, and countries for purposes of identifying and, where appropriate, reporting activities that we suspect may involve possibleterrorist activity or money laundering.

Prior to sharing information and annually thereafter, the Palomar Corporate Compliance Department ("Corporate Compliance") will oversee the filing of the "Notification for Purposes of Section 314(b) of the USA Patriot Act and 31 CFR 1025.540" for Minnesota Life, Securian Life Insurance Company,and Securian Funds Trust (formerly, Advantus Series Fund, Inc.). Other applicable subsidiaries under Palomar Group, Inc. are responsible for filing the appropriate notification and for providing theCompliance Manager confirmation of such filing.

Before Palomar shares information with another financial institution, Palomar will take reasonable steps to verify that the other financial institution has submitted the requisite notice to FinCEN,either by obtaining confirmation from the financial institution or by consulting a list of such financial institutions that FinCEN will make available. Palomar understands that this requirement applieseven to financial institutions with which we are affiliated and that we will obtain the requisite notices from affiliates and follow all required procedures. Requests for information sharing from a financial institution that is not affiliated with Palomar should be referred to the AML Compliance Officer.

Palomar will employ appropriate procedures both to ensure that only relevant information is shared and to protect the security and confidentiality of this information, including segregating it from Palomar's other books and records.

Palomar will also employ procedures to ensure that any information received from another financial institution shall not be used for any purpose other than:

- Identifying and, where appropriate, reporting on money laundering or terrorist activities.
- Determining whether to establish or maintain an account, or to engage in a transaction.
- Assisting the financial institution in complying with performing such activities.

Joint Filing of SARs by Broker-Dealers and Other Financial Institutions

Palomar will file a joint SAR if Palomar and another financial institution that is subjectto the SAR regulations are involved in the same suspicious transaction. For example, Palomar and Palomar Services, Inc. (SFS) may file one SAR with respect to suspicious activity involving the sale of variable insurance products. If a joint SAR is filed, Palomar will maintain a copy of theSAR and supporting documentation in accordance with BSA recordkeeping requirements.

If Palomar determines it is appropriate to jointly file a SAR, we understand that we cannot disclose that we have filed a SAR to any financial institution except the financial institution that is filing jointly. If we determine it is not appropriate to file jointly, we understand that we cannot disclose that we have filed a SAR to any other financial institution or insurance company.

Comparison with Government Lists

Comparison with the Office of Foreign Assets Control's SDN Lists

Palomar will check to ensure that none of its applicable customers appear on the SDN list and are not engaging in transactions that are prohibited by the economic sanctions and embargoes administered andenforced by the Office of Foreign Assets Control (OFAC). Generally, Palomar will scan the customer against the SDN list prior to opening an account and quarterly thereafter. Palomar will access the SDN list through a software program to ensure speed and accuracy. Because the SDN list and listings of economic sanctions and embargoes are updated frequently, Palomar will subscribe toreceive available updates when they occur.

Palomar may rely on the performance of OFAC scans by a vendor or another financial institution before an account is opened when such reliance is reasonable under the circumstances.

If Palomar determines that a customer is on the SDN list or is engaging in transactions that are prohibited by the economic sanctions and embargoes administered and enforced by OFAC, Palomar will reject the transaction and/or block the customer's assets and file a blocked assets and/or rejected transaction form with OFAC within 10 days. Palomar will also call the OFAC Hotline at or use OFAC's e-hotline.

Comparison with Government-provided Lists of Terrorists

When Palomar receives notice that a federal government agency has issued a list of known or suspected terrorists and identified the list as a list for Customer Identification Program purposes, Palomar will, within a reasonable period after an account is opened (or earlier if required by another federal law, regulation or federal directive issued in connection with an applicable list), determine whether a customer appears on any such list of known or suspected terrorist organizations issued by anyfederal government agency and designated as such by Treasury in consultation with federal functional regulators. Palomar will follow all federal directives issued in connection with such lists.

Palomar will continue to comply separately with OFAC rules prohibiting transactions with certain foreign countries or their nationals.

Know Your Customer

Customer Due Diligence

Customer Due Diligence (CDD) and Enhanced Due Diligence are the foundation of a strong AML compliance program. Palomar performs CDD as part of the underwriting and suitability review processes for new product that have a cash value or investment features.

At a minimum, for these products Palomar collects the following information:

- The purpose of the account.
- The source of funds and wealth.
- The beneficial owners of the accounts.
- The customer's occupation or type of business.

Based on this information, Palomar can determine the customer's anticipated account activity including volume and type of transactions.

The CDD information is reviewed in connection with, and will provide a baseline for, evaluating customertransactions to determine whether the transactions are suspicious and need to be reported.

In certain circumstances, Palomar may perform enhanced due diligence. Such circumstances include, but are not limited to, identification of red flags, requests for contracts in excess of established limits and instances in which the customer does not match the target market for a product.

Correspondent Accounts for Foreign Shell Banks

Palomar does not establish, maintain, administer, or manage correspondent accounts for foreign banks. A "correspondent account" is an account established by a financial institution for a foreign bank to receive deposits from; or to make payments or other disbursements on behalf of the foreign bank;or to handle other financial transactions related to the foreign bank.

Palomar is aware that a financial institution is prohibited from establishing, maintaining, administering, or managing a correspondent account for, or on behalf of, a foreign shell bank.

On an annual basis the AML Compliance Officer will review the company's products to ensure no changeshave occurred that would allow such accounts to be opened or maintained. Upon finding or suspecting such accounts, Palomar associates must notify the AML Compliance Officer, who will terminateany verified correspondent accounts in the United States for a foreign shell bank. Palomar will also terminate any correspondent account that Palomar determines is not maintained by a foreign shell bank but is being used to provide services to such a shell bank. Palomar will exercise caution regarding liquidating positions in such accounts and take reasonable steps to ensure that no newpositions are established in such accounts during the termination period. Palomar will terminate any correspondent account for which we have not obtained the information required in the regulations regarding shell banks within the time periods specified in those regulations.

Although Palomar does not maintain any accounts, including correspondent accounts, with any foreign jurisdiction or financial institution, if FinCEN issues a final rule imposing a special measure against one or more foreign jurisdictions or financial institutions, classes or international

transactions or types ofaccounts deeming them to be of primary money laundering concern, we understand that we must read FinCEN's final rule and follow any prescriptions or prohibitions contained in that rule.

Private Banking Accounts for Non-U.S. Persons

Palomar does not establish, maintain, administer, or manage private banking accounts. A "private banking" account is an account that requires a minimum aggregate deposit of $1 million, is established for one or more individuals and is assigned to or administered by an officer, employee, or agent of a financial institution acting as a liaison between the financial institution and the direct or beneficial owner of the account.

Palomar is aware that due diligence must be performed on all private banking accounts. In addition, enhanced due diligence must be conducted to detect and report transactions that may involve money laundering or the proceeds of foreign corruption.

On an annual basis the AML Compliance Officer will review the company's products to ensure no changeshave occurred that would allow such accounts to be opened or maintained. In the event such an accountis discovered, Palomar will conduct due diligence on the account.

This due diligence will include at least:

- Ascertaining the identity of all nominal holders and holders of any beneficial ownership interestin the account (including information on those holders' lines of business and sources of wealth).
- Ascertaining the source of funds deposited into the account.
- Ascertaining whether any such holder may be a senior foreign political figure.
- Detecting and reporting, in accordance with applicable laws and regulations, any known orsuspected money laundering, or use of the proceeds of foreign corruption.

If due diligence (or the required due diligence, if the account holder is senior foreign political figure) cannot be performed adequately, the AML Compliance Officer will determine whether to not open the account, suspend the transaction activity, file a SAR or close the account.

Suspicious Activity Monitoring

The detection and reporting of suspicious activity are keys to the deterrence of money laundering and terrorist activity.

Palomar monitors account activity for unusual size, volume, pattern, or type of transactions, taking into account risk factors and red flags that are appropriate to our business. Monitoring is conducted by associates in the business units manually reviewing transactions for suspicious customer behavior andtransaction activity, including but not limited to, examples of money laundering red flag activity providedin Exhibit A. An associate who detects suspicious activity will bring it to the attention of their supervisor who will consult with the AML Compliance Officer or their designee.

The AML Compliance Officer or a designee will conduct reviews of potentially suspicious activity detectedby the business units. The AML Compliance Officer or a designee will conduct an appropriate investigationand review relevant information from internal or third-party sources before

a SAR is filed. Relevant information can include, but not be limited to, the following: banking information, source of funds verification, financial/estate planning documentation, and business information.

The AML Compliance Officer or a designee is responsible for monitoring the business unit's review of anyactivity that is detected as possibly suspicious. The AML Compliance Officer or a designee will also determine whether additional steps are required, will document when and how this monitoring is carriedout, and will report suspicious activities to the appropriate authorities.

Emergency Notification to the Government by Telephone

Certain suspicious activities require immediate telephone reporting of the transaction. These situations include but are not limited to instances when:

- A customer's name is on the OFAC list.
- A customer tries to use bribery, coercion, or similar means to open an Account or carry out asuspicious activity.
- Palomar has reason to believe a customer is trying to move illicit cash out of the government's reach.
- Palomar has reason to believe a customer is about to use the funds to further an act of terrorism.

Palomar will call one or more of the following:

- OFAC Hotline.
- FinCEN's Department's Financial Institutions Hotline.
- Local United States Attorney's Office.
- Local FBI Office.
- Local SEC Office.

Although not required, in cases where Palomar has filed a SAR that may require immediate attention by the SEC, we may contact the SEC via the SEC SAR Alert Message Line to alert the SEC to the filing. Palomar understands that calling the SEC SAR Alert Message Line does not alleviate our obligation to file a SAR or notify an appropriate law enforcement authority.

Suspicious Activity and BSA Reporting

Suspicious Activity Report Filing

Palomar will report to FinCEN any transaction that, alone or in the aggregate, involves at least

$5,000 in funds or other assets, and Palomar knows, suspects, or has reason to suspect that itfalls within one of following classes:

- The transaction involves funds derived from illegal activity or is intended or conducted to hide ordisguise funds or assets derived from illegal activity.
- The transaction is designed, whether through structuring or other means, to evade the requirements of the BSA.

- The transaction appears to serve no business purpose or apparent lawful purpose or is not the sort of transaction in which the customer would be expected to engage and for which Palomar knows of no reasonable explanation after examining the available facts.

The above guidelines extend to patterns of transactions. Therefore, if Palomar determines thata series of transactions would not independently trigger suspicion, but when taken together, form a suspicious pattern of activity, Palomar will file a SAR. Also, if a transaction doesn't meet a specific dollar threshold that would trigger the filing of a SAR, but does raise an identifiable suspicion of criminal,terrorist, or corrupt activities, Palomar will appropriately review the transaction and determineif a SAR should be filed.

Palomar will also file a SAR and notify the appropriate law enforcement authority in situations involving violations that require immediate attention, such as terrorist financing or ongoing money laundering schemes.

Palomar may file a SAR for any suspicious transaction that we believe is relevant to the possible violation of any law or regulation but that is not required to be reported under the SAR rule.

Palomar will report suspicious transactions by completing a SAR and will collect and maintain supporting documentation as required by the BSA regulations. We will file a SAR no later than 30 calendardays after the date of the initial detection of the facts that constitute a basis for filing a SAR. If no suspectis identified on the date of the initial detection, we may delay filing the SAR for an additional 30 calendardays pending identification of a suspect, but in no case will the reporting be delayed more than 60 calendar days after the date of initial detection. The phrase "initial detection" does not mean the momenta transaction is identified for review. The 30-day (or 60-day) period begins when an appropriate review isconducted, and a determination is made that the transaction under review is "suspicious" within the meaning of the SAR requirements. A review must be initiated promptly upon identification of unusual activity that warrants investigation.

Generally, Palomar will report any continuing suspicious activity on a previously filed SAR with a new filing at least every 90 days. Palomar will continue to assess whether it should continue to maintain the account or effect the transaction in question.

Palomar will retain copies of any SAR filed and the original or business record equivalent of any supporting documentation for at least five years from the date of filing the SAR. We will identify and maintain supporting documentation and make such information available to FinCEN, the SEC or any otherappropriate law enforcement agencies upon request.

Palomar will not notify any person involved in the transaction that the transaction has been reported, except as permitted by BSA regulations. In the event Palomar is subpoenaed or required to disclose a SAR or the information contained in the SAR, we will decline to produce the SAR and any information that would disclose that an SAR was prepared or filed, except where disclosures arerequested by FinCEN, the SEC or another appropriate law enforcement or regulatory agency. Palomar will notify FinCEN of any such request and our response.

Exceptions to Filing a Suspicious Activity Report

Palomar is not required to file a SAR to report as the result of:

- A robbery or burglary that is reported by Palomar to appropriate law enforcement authorities.
- Lost, missing, counterfeit, or stolen securities with respect to which Palomar files a report pursuant to the reporting requirements of 17 CFR 240.17f-1.

- A violation of the federal securities laws or rules of a self-regulatory organization by Palomar, its officers, or associates, that is reported appropriately to the SEC or self-regulatory organization, except for a violation of Rule 17a-8 under the Securities Exchange Act of 1934, whichmust be reported on a SAR.

State Reporting Requirements

Certain states have enacted their own reporting requirements which may or may not be satisfied by reporting to the federal government. Consequently, whenever any type of transaction report under the BSA is filed with the federal government, Palomar will undertake efforts to analyze relevant state law to determine whether a duplicate or comparable form needs to be filed with a state authority.

Safe Harbor Provisions

Federal law provides broad "safe harbor" protection from civil liability for the filing of SARs to report suspected or known criminal violations and suspicious activities, regardless of whether such reporting is mandatory or is done on a purely voluntary basis. The BSA provides that a financial institution and its directors, officers, associates, and agents who file a SAR "shall not be liable to any person" for such disclosure or for any failure to notify the person involved in the transaction or any other person of such disclosure.

Form 8300

Palomar's Monetary Instruments Policy prohibits the receipt of cash and currency as defined in the instructions for Form 8300 reporting. If Palomar discovers such transactions have occurred, Palomar will file a Form 8300 with FinCEN for currency transactions that exceed $10,000. Palomar will treat multiple transactions involving currency as a single transaction for purposes of determining whether to file a Form 8300 if the transactions total more than $10,000 and are made by or on behalf of the same person during any one business day.

Although Palomar does not accept currency, cashier's checks are accepted. Cashier's checks in amounts less than $10,000 are tracked. Palomar will file a Form 8300 or SAR if we know the payer is trying to avoid the reporting of such a transaction on Form 8300.

Currency and Monetary Instrument Transportation Reports (CMIR)

Palomar's Monetary Instruments Policy prohibits the receipt of currency. Palomar willfile a Currency and Monetary Instrument Transportation Report (CMIR) with the Commissioner of Customs if we discover that we have received or caused or attempted to receive from outside of the United States, currency or other monetary instruments in an aggregate amount exceeding $10,000 at one time. We will also file a CMIR if we discover that we have physically transported, mailed or shipped or caused or attempted to physically transport, mail or ship by any means other than through the postal service or by common carrier, currency or other monetary instruments of more than $10,000 at one time.

Report of Foreign Bank and Financial Accounts (FBAR)

Palomar will file a Report of Foreign Bank and Financial Accounts for any financial accounts in a foreign country of more than $10,000 that we hold, or for which we have signature authority over.

Wire Transfers of $3,000 or More Under the "Joint and Travel Rule"

Palomar does not issue bank checks or drafts, cashier's checks, money orders or traveler's checksin the amount of $3,000 or more.

Palomar

Under Treasury's Joint and Travel rule, when Palomar wire transfers funds, Palomar will create a paper trail by which enforcement officials can trace the transfer of such funds. At a minimum,Palomar will record in writing the following information:

- Name and address of the sender and recipient
- Amount of the transmittal
- Identity of recipient's financial institution
- Account number of the recipient
- Date of the transaction

AML Recordkeeping

Responsibility for Required AML Records and SAR Filings

Palomar's AML Compliance Officer is responsible for ensuring that the AML records are maintained properly, and that SARs are filed as required.

In addition, as part of our AML program, Securian will create and maintain SARs, Form 8300s, CMIRs, FBARs and relevant documentation on funds transmittals. We will maintain SAR and accompanying documentation for at least five years. ML/SL will maintain other documents according to existing

BSA and other recordkeeping requirements, including certain SEC rules that require six-year retention periods and Palomars Information Governance Program.

SAR Maintenance and Confidentiality

Palomar will hold SARs and any supporting documentation confidential. We will not inform anyone outside of FinCEN, the SEC, or other appropriate law enforcement or regulatory agency about a SAR filing. We will refuse any subpoena requests for SARs or for information that would disclose that a SAR has been prepared or filed. Palomar will notify FinCEN of any such subpoena requests thatare received. We will segregate SAR filings and copies of supporting documentation from other books andrecords to avoid disclosing SAR filings. Palomars AML Compliance Officer will handle all subpoenas or other requests for SARs. We may share information with another financial institution aboutsuspicious transactions to determine whether to file a joint SAR. In cases in which we file a joint SAR for atransaction that has been handled by ML/SL and another financial institution, both financial institutions will maintain a copy of the filed SAR.

It is our policy that all SARs will be reported to the Chief Legal Officer regularly with a clear reminder of the need to maintain the confidentiality of the SAR.

Associate Training

The Palomar AML Program training is developed and maintained under the leadership of the AML Compliance Officer and/or designee and meets the following requirements:

- Occurs at least annually.
- Is required for all associates with administrative responsibility for covered products.

- Is reviewed and updated as necessary, to reflect new developments in the regulation.
- Documentation evidencing completion of training is maintained in accordance with recordsretention requirements.
- Is included in the scope of the periodic (commensurate with the risks posed by Palomar's covered products) AML audit conducted by the Internal Audit Department.

Associates whose job responsibilities require AML training may include, but are not limited to, associateswho open accounts, handle client checks or wire transfers, or process client transactions, and associates who supervise such associates.

Training Program Content

Palomar's AML Training Program includes, but is not limited to, information that provides an understanding of money laundering activities, prevention and detection methods, and regulatory requirements. Basic AML training content includes:

- How to identify red flags and signs of money laundering that may arise during the employee'sduties.
- What to do once the risk is identified (including how, when and to whom to escalate unusualcustomer activity or other red flags for analysis).
- The employees' role in the AML Compliance program and how to perform them.
- The disciplinary consequences including civil and criminal penalties for noncompliance with theBSA.

The development of AML training may be delegated to appropriate persons selected by the Palomar AML Compliance Officer. Specialized content will be identified and may be developed by management of the areas in need of such training.

Training Program Implementation

Training records will be maintained in accordance with the Palomar Records Retention Schedule.

Delivery of AML training may be through on-line industry courses, web-ex, educational pamphlets, videos,intranet systems, in-person lectures, explanatory memos and other methods.

Independent Testing

The audit of Palomar's AML program will be performed periodically, commensurate with the risks posed by Palomar's covered products, by the Internal Audit Department in coordination with the Anti-Fraud and Financial Crimes team and may include:

- Evaluating the overall integrity and effectiveness of Palomar's AML Compliance Program.
- Evaluating Palomar's procedures for BSA reporting and recordkeeping requirements.
- Evaluating internal monitoring program and, if necessary, perform additional testing of Palomar's transactions with an emphasis on high-risk areas.
- Evaluating adequacy of training programs.
- Evaluating process for identifying suspicious activity.

- Evaluating process for reporting suspicious activity.
- Evaluating policy for reviewing accounts that generate multiple SAR filings.
- Evaluating Palomar's response to previously identified deficiencies.

The scope of the audit will be determined by the Internal Audit Department. Audit findings, including recommendations to remedy any deficiencies, will be reported to the Palomar AML Compliance Officer. The Palomar AML Compliance Officer will be responsible for evaluating and implementing any recommendations and will have final approval authority over action dates and assignments established in response to Audit Improvement Agreements. The Palomar AML Compliance Officer will also determine additional distribution of the final audit report.

Confidential Reporting of AML Non-Compliance

Palomar associates will report any violations of Palomar's AML Program to the AML Compliance Officer, unless the violations implicate the AML Compliance Officer, in which case the associate shall report to the Palomar Chief Legal Officer. Such reports will be confidential,and the associate will suffer no retaliation for making them.

Senior Management Approval of AML Program

The AML Compliance Officer has approved the AML Compliance Program as reasonably designed to achieve and monitor ML's ongoing compliance with the requirements of the BSA and its implementing regulations.

The Chief Legal Officer will be provided a copy of the AML Program document periodically, at least every three years or upon substantive revision. The AML Compliance Officer will consider program revisions, if any, as suggested by the Chief Legal Officer.

Exhibits

Exhibit A – Money Laundering Red Flags

Certain red flags may signal possible money laundering or terrorist financing activities. The following list of money laundering and terrorist financing red flags may be noted at the point of sale or while processinga transaction. Their presence may indicate the need to notify the Palomar AML Compliance Officer to determine if the situation warrants further investigation and possible filing of a SAR.

Customer Identity Red Flags

- Legal entity is known to be associated with a terrorist organization or conducts business in a jurisdiction that has been designated by the U.S. as a primary money laundering concern or has been designated as non-cooperative by an international body.
- The customer is from or has accounts in a country identified as a non-cooperative country or territory.
- There is overlap between corporate officers or other identifiable similarities associated with addresses, references, and anticipated financial activities.
- The customer gives a false or stolen SSN.
- The customer (or a person publicly associated with the customer) has a questionable backgroundor is the subject of news reports indicating possible criminal, civil, or regulatory violations.

Reason for Opening the Account Red Flags

- The customer exhibits unusual concern about Palomar's compliance with government reporting requirements and Palomar's AML policies (particularly concerning their identity, types of business and assets), or is reluctant or refuses to reveal any information concerning business activities or furnishes unusual or suspicious identification or business documents;
- The customer wishes to engage in transactions that lack business sense or apparent investment strategy or are inconsistent with the customer's stated business or investment strategy.
- The occupation stated by the customer is not commensurate with the level or type of potential activity for the account.
- Unexplained inconsistencies of data are noted during the process of identifying or verifying a customer.
- The purpose for opening an account for non-profit or charitable organization appears to have noeconomic purpose or link between the stated mission of the organization and other parties to thetransaction.

Customer Behavior Red Flags

- The customer exhibits a lack of concern regarding risks, commission, or other transaction costs.
- The customer appears to be acting as an agent for an undisclosed principal, but declines or is reluctant, without legitimate commercial reasons, to provide information or is otherwise evasiveregarding that person or entity.
- The customer has difficulty describing the nature of his or her business or lacks general knowledgeof his or her industry.
- The customer makes an unusual request, such as asking for help in converting cash into checks.
- The customer is always in a rush.
- The customer requests that the account opening transaction be processed to avoid Palomar's normal documentation requirements.
- The customer maintains multiple accounts or maintains accounts in the names of family membersor corporate entities, for no apparent purpose.
- The customer seeks to change or cancel a transaction after being informed that a report will befiled or that information will need to be verified.
- The customer conducts its business under unusual circumstances, at irregular hours or in unusuallocations.
- The customer offers gifts or gratuities greater than Palomar's policies allow after being informed of Palomar's policies.
- The customer (or someone connected with the account) is the subject of news reports or rumorsindicating possible criminal regulatory, or civil fraud violations.

- The customer (or someone connected with the account) is the subject of inquiry or investigationby a regulatory or criminal prosecutorial agency.

Customer Transaction Red Flags

- A customer who borrows the maximum amount soon after purchasing the product.
- The customer engages in excessive journal entries between unrelated accounts with no apparentbusiness purpose.
- The customer makes deposits or premium payments with multiple monetary instruments purchased from the same and/or different financial institutions.
- The customer engages in transactions involving cash or cash equivalents or other monetary instruments that appear to be structured to avoid the $10,000 government reporting requirements, especially if the cash or monetary instruments are in an amount just below reporting or recording thresholds.
- The customer account has unexplained or sudden extensive wire activity, where previously therehad been little or no wire activity.
- The customer makes a fund deposit followed by an immediate request that the money be withdrawn or transferred to a third party, or to another business without any apparent business reason.
- The customer's transactions are unusual or inconsistent with the customer's normal trading practices.
- The customer makes investments that do not make economic sense, such as large sums sitting ina money market account.

Source of Funds Red Flags

- Unexplained or negotiation of third-party checks.
- The source of funds is suspicious such as transfers from a bank or other type of account that donot appear to have a legitimate relationship with the business.
- The customer's source of funds or other assets appear to be well beyond the resources of theperson or entity.
- The information provided by the customer that identifies legitimate sources for funds is false,misleading, or substantially incorrect.
- Upon request, the customer refuses to identify or fails to indicate any legitimate source for fundsand other assets.

Palomar

Definitions

The following terms and their definitions are used throughout this AML Program:

- Customer(s) shall include, but is not limited to client, accountholder, insured, policyowner in relation to any insurance products with cash value and investment features.
- Associate shall include all employees of Palomar.
- Account shall include but is not limited to insurance policy or annuity contract.
- Transaction shall include but is not limited to deposits of money to pay premiums, deposits of contributions, withdrawals, or liquidations of funds from an insurance policy, annuity contract or account, or other monetary activities related to an account, policy or contract
- We refers to Palomar
- Money Laundering Defined
    - Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the unlawful proceeds appear to have been derived from legitimate origins or constitute legitimate assets. Generally, money laundering occurs in three stages. Cash first enters the financial system at the “placement” stage, where the cash generated from criminal activities is converted into monetary instruments, such as money orders, traveler’s checks, cashier’s checks, or deposited into accounts at financial institutions.
    - At the “layering” stage, the funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin. At the “integration” stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses.
    - Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal either the origin of funds or their intended use, which could be for criminal purposes. Legitimate sources of funds are a key difference between terrorist financiers and criminal organizations. In addition to charitable donations, legitimate sources include foreign government sponsors, business ownership, and personal employment. Although the motivation differs between traditional money launderers and terrorist financiers, the actual methods used to fund terrorist operations can be the same as or like methods used by other criminals to launder funds. Funding for terrorist attacks does not require large sums of money and the associated transactions may not be complex.