MUTUAL TRUST LIFE INSURANCE COMPANY,
A PAN-AMERICAN LIFE INSURANCE GROUP STOCK COMPANY
Compliance Plan
Economic Sanction, Foreign Assets Control and Money Laundering Abatement Laws

I. POLICY STATEMENT

It is the policy of Mutual Trust Life Insurance Company, A Pan-American Life Insurance Group Stock Company ("Mutual Trust") to comply fully with all applicable U.S. economic sanctions, foreign asset control and money laundering abatement laws and regulations. Mutual Trust (also referred to as "Company", "Firm" and "We") is committed to maintaining company wide awareness of the importance of these laws and regulations and has developed this Compliance Plan, providing direction with respect to compliance activities and setting forth internal policies, procedures and controls to ensure compliance with applicable U.S. laws and regulations pertaining to economic sanctions, foreign asset control and money laundering abatement.

It is the policy of the Company to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities. 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 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 or traveler'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 the origin or intended use of the funds, which will later be used for criminal purposes.

II. OVERVIEW OF RELEVANT LAWS AND REGULATIONS

The Department of the Treasury issued a Final Rule applicable for insurance companies on May 2, 2006 (Federal Register / Vol. 70, 212 31 CFR Part 103, Financial Crimes Enforcement Network; Amendment to the Bank Secrecy Act Regulations—Anti-Money Laundering Programs for Insurance Companies). The Financial Crimes Enforcement Network (FinCEN) issued the final rule to prescribe minimum standards applicable to insurance companies pursuant to the provision in the Bank Secrecy Act that requires financial institutions to establish anti-money laundering programs. The United States imposes economic sanctions and trade embargoes to further U.S. foreign policy and national security objectives. For example, the Department of the Treasury's Office of Foreign Assets Control ("OFAC") administers economic sanctions programs created

pursuant to Executive Orders, laws and regulations. Economic sanctions laws are broadly written and may vary significantly depending on the country involved. U.S. economic sanctions and foreign assets control laws generally prohibit individual U.S. citizens, permanent residents and U.S. corporations from engaging in most types of transactions involving risks, insurers, individuals or other entities from "Sanctioned Countries" and with individuals and entities on the "Specially Designated Nationals" list (see below for the definition of those terms).

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ("USA PATRIOT Act") was signed into law on October 26, 2001. Title III of the USA PATRIOT Act, which may by cited as the International Money Laundering Abatement and Financial Anti-Terrorism Act of 2001 ("IMLAFATA"), provides the Secretary of the Treasury and other departments and agencies of the federal government with enhanced authority to identify, deter and punish international money laundering activities. In this connection, the Bank Secrecy Act and the Currency and Foreign Transactions Reporting Act of 1970 previously set forth certain reporting and recordkeeping requirements for currency and foreign transactions. Patterns of currency transactions that are less than the reporting requirement but in aggregate exceed it may also be subject to certain filing requirements.

A. Sanctioned Countries

The "Sanctioned Countries" are those jurisdictions subject to U.S. economic sanctions and foreign assets control laws. U.S. economic sanctions laws generally are territorial in nature, with certain exceptions, and may apply to an entire country, a constituent part of the country, or to a specific regime or a political movement within a country.

Based on changing foreign policy objectives and national security needs, the list of Sanctioned Countries is revised periodically to add new jurisdictions subject to sanctions or to remove jurisdictions no longer sanctioned. These changes generally are effective immediately upon announcement. Therefore, business personnel making decisions on underwriting, accepting premiums, and paying claims must stay currently informed of changes, through the activities described in this Compliance Plan.

B. Specially Designated Nationals

The "Specially Designated Nationals" are the individuals and entities that have been designated by the United States Government as being affiliates or agents of current or prior Sanctioned Country Governments or as being engaged in certain illicit activities, such as narcotics trafficking or terrorism. As such, they are subject to U.S. economic sanctions and foreign asset control laws. Additional individuals and entities are added to, or removed from, this list continuously.

Due to frequent changes to the list of Specially Designated Nationals, business personnel making decisions on underwriting, accepting premiums and paying claims

must stay currently informed of changes, through the activities described in this Compliance Plan.

III. MUTUAL TRUST RISK IDENTIFICATION

***Geographies*:** Mutual Trust is licensed to do business in 49 states and Puerto Rico, including states that border other countries. As a result, Mutual Trust conducts an analysis of its money laundering risk resulting from the states in which it does business. This risk assessment is memorialized on a separate and distinct document. It is conducted every year.

Customer Types: Mutual Trust's typical customers are individuals who wish to take advantage of the full benefits of Participating Whole Life Insurance Products. These are generally financially secure individuals who maintain the flexibility of envisioning Mutual Trust's products as a benefit that far exceeds the death benefit aspect of them. They often look to actively take advantage of a policy's "living benefits," such as cash values. However, Mutual Trust recognizes the risks that are associated with the customers it has. As a result, Mutual Trust conducts an analysis of its money laundering risk resulting from the various customers that purchase its products. This risk assessment is memorialized on a separate and distinct document. It is conducted every year.

Products: Mutual Trust markets Whole Life, Universal Life, Blended Life, Term Life and Annuity Products. However, Mutual Trust's sale of annuity products is very minimal. The vast majority of its sales relate to its whole life products. Mutual Trust recognizes that the associated money laundering risk may change depending on the type of product sold and the method in which it operates. As a result, Mutual Trust conducts an analysis of its money laundering risk resulting from the products it sells. This risk assessment is memorialized on a separate and distinct document. It is conducted every year.

Distribution Channels: Mutual Trust utilizes only one distribution channel to market its products and that is through the use of independent agents. The risk of adding this party to the sales process is assessed by Mutual Trust on an annual basis. This risk assessment is memorialized on a separate and distinct document. It is conducted every year.

Fund Flows: Mutual Trust's normal business practices include the flow of funds, both in and out of Mutual Trust. This consistent stream of funds can potentially become an environment ripe for money laundering abuse. As a result, Mutual Trust conducts an analysis of its money laundering risk resulting from its receipt and payment of funds. This risk assessment is memorialized on a separate and distinct document. It is conducted every year.

IV. COMPLIANCE

A. Customer Due Diligence

1. Customer Identification Program

Mutual Trust adopted a Customer Identification Program (CIP), effective October 1, 2003. In recognition that Mutual Trust's independent agency force stands in a unique position to view the applicant and note any unusual or suspicious behavior, it has adopted a CIP requiring agents to take reasonable steps to attempt to verify the applicant's identity.

Thus, Mutual Trust agents secure and record the social security number of all United States citizens. If the applicant is not a United States citizen, the agent is required to obtain and record, in the following order of preference: (i) the applicant's social security number, (ii) alien identification number, or (iii) passport number along with the country of issuance. The information secured must be included on the insurance application when it is submitted.

In addition to the above-mentioned information, the agent is responsible for observing an acceptable identification card whenever he or she meets with the customer. An acceptable identification card is an unexpired document containing a photo of the applicant. The agent will first attempt to review a government issued identification card such as a driver's license, state identification card, or passport, if possible. If, for some justifiable reason the applicant does not have any of this information, the agent will review alternative forms of identification such as a school or company identification card. Finally, a street address is needed for every customer.

All applicant information obtained by the agent is secured in the spirit of attempting to verify the identity of the applicant. If the agent cannot verify the applicant's identity, the insurance application should not be taken. If the applicant's documentation, behavior, or representations cause the agent to become suspicious of the applicant's identity or intentions, the agent must report his or her suspicions to Mutual Trust immediately.

Mutual Trust also has adopted GIACT, which is a vendor that confirms the authenticity of reported bank accounts. It is thru this service that Mutual Trust can confirm that a bank account belongs to a policyholder or beneficiary prior to depositing funds into that account. This process greatly reduces the risk of fraud.

2. Beneficial Ownership

Mutual Trust adopted processes so as to collect beneficial ownership information whenever a legal entity is involved in the purchase of a Mutual Trust product. A legal entity includes a corporation, limited liability company, or other entity that is created by a filing of a public document with a Secretary of State or similar office, a general partnership, and any similar business entity formed in the United States or a foreign country. A legal entity is not a proprietorship, unincorporated associations, or natural persons opening accounts on their own behalf.

As a part of these processes, Mutual Trust will require certain policy owner information at the time that an application is taken or if a current policy undergoes an ownership change indicative of new ownership to a corporation, limited liability company, or other entity that is created by a filing of a public document with a Secretary of State or similar office, a general partnership, and any similar business entity formed in the United States or a foreign country. Mutual Trust producers will have to secure this additional information whenever the policy owner is a company or other legal entity. The information will include:

i) Any person who directly or indirectly, owns 25% or more of equity interest in the company or legal entity; and
ii) A single individual who has significant responsibility to control, manage, or direct a legal entity.

The information will be secured by the producer on a specially designed form modeled from a specimen form issued by FINCEN. No application will be approved without the proper completion of this form. The individuals identified on this form will be OFAC checked by Mutual Trust's Patriot Manager administrative system.

3. Purpose of Client Relationships

Mutual Trust recognizes that its clients purchase its products for different reasons and purposes. For example, some clients may purchase a life insurance product for the death benefit while others may purchase it to creatively utilize the living benefits of the policy. Due to the smaller size of the company and the limited amount of products offered by the company, Mutual Trust does not believe it would be a high priority target for money launderers. However, as a precaution, Mutual Trust has created a customer risk profile to help in its attempt to identify any illegal activities.

As a part of the application process, Mutual Trust secures personal identifying information from its applicants such as name, address, social security number, driver's license state and number, email address and beneficiary name and address. Also, Mutual Trust requires that the selling producer include information on an Agent's Report so that it can better understand the nature and purpose of the financial purchase. Furthermore, the applicant's name is automatically inputted into the company's Patriot Manager administrative system so as to OFAC check the applicant's name. No application will be approved and all required reporting will be executed if there is an OFAC "hit" when the

applicant's name is inputted into the Patriot Manager system. This individual would automatically be treated as a high risk for illegal activity.

Furthermore, Mutual Trust will consider any type of producer observations of a suspicious nature when considering whether to treat an applicant as meeting a high risk profile.

Some additional red flags that would cause Mutual Trust to treat an applicant as a high risk for illegal activity include:

- The proposed owner is a business that is suspicious in nature either by the method in which it was set-up, the apparent lack of needed personnel, the location of business activities, or the types of products or services it provides;
- Policy owner association with certain countries;
- Uncertain relationships between parties to the contract;
- The purchase of the Mutual Trust product appears to be inconsistent with the customer's needs;
- The customer exhibits unusual concern about the company's compliance with government reporting requirements and the company's anti-money laundering policies, particularly regarding his or her identity, type of business and assets, or is reluctant or refuses to reveal any information concerning business activities, or furnishes unusual or suspect identification or business documents;
- The information provided by the customer that identifies a legitimate source of funds is false, misleading, or substantially incorrect;
- The customer provides an incorrect address;
- The stated purpose of the purchase of insurance is suspicious;
- Upon request, the customer refuses to identify or fails to indicate any legitimate source for his or her funds or other assets;
- The customer (or a person publicly associated with the customer) has a questionable background or is the subject of news reports indicating possible criminal, civil, or regulatory violations;
- The customer exhibits a lack of concern regarding risks, commissions, or other transaction costs;
- The customer appears to be acting as an agent for an undisclosed party but declines or is reluctant, without any apparent or obvious reason, to provide information or is otherwise evasive regarding that party;
- The customer has difficulty describing the nature of his or her business or lacks general knowledge of his or her industry;
- The customer is from, or has accounts in, a country identified as a noncooperative country or territory;
- The customer maintains multiple accounts, or maintains accounts in the names of family members or corporate entities, for no apparent purpose; and
- The reluctance by a customer to provide identifying information when purchasing an insurance product or the providing of minimal or seemingly fictitious information.

Any Mutual Trust representative identifying a high risk factor that would trigger a high risk classification is required to report the matter to his or her manager in conjunction with notification to the AML Compliance Officer immediately.

4. On-Going Monitoring of Suspicious Transactions

Mutual Trust utilizes Patriot Manager as its administrative system to alert the company to any suspicious actions taken on an issued policy. Each day, Mutual Trust's Law Department is alerted to potential suspicious activity. Law Department personnel thoroughly review these alerts to determine if there is any indication of wrongdoing. The alerts are triggered by the company's establishment of preset guidelines so as to determine the type of activity that would be deemed suspicious. A record is maintained that an alert was reviewed and addressed along with the reason for the method in which it was handled.

In addition, company personnel will immediately alert their manager in conjunction with the AML Compliance Officer of any suspicious activity relating to the type of funds received, attempted changes in policy ownership, policy loans and attempted beneficiary changes or any other suspicious activity they encounter. Upon receiving notice of the suspicious activity, the AML Compliance Officer will conduct a complete investigation and comply with any reporting requirements.

Pan-American Life Insurance Company (PALIC) currently utilizes Bridger as its administrative system to review US policy activity for potential ant-money laundering behavior but is in the process of transitioning to the FISERV administrative system. Monthly reports surrounding this activity on U.S. Life business is provided monthly to Mutual Trust's AML Compliance Officer for review. Mutual Trust is being included on any reports of suspicious activity relating to U.S. Policies sold to foreign individuals, including, Politically Exposed Person Reports and follow-ups.

B. Procedures to Prevent and Mitigate Identity Theft: Red Flags

Mutual Trust relies on certain indicators in its attempts to identify situations where an applicant or any other party involved in an insurance transaction or maintaining a relationship with Mutual Trust attempts to hide his or her identity or otherwise mislead Mutual Trust about his or her identity. These indicators may include the following:

- Agent failure to obtain evidence of identification;
- Agent disclosure to Mutual Trust of applicant's suspicious behavior;
- An alert issued by Mutual Trust's Patriot Manager Software System is triggered upon receipt of the application;
- Identification presented appeared to be altered or forged;
- The person providing picture identification does not look like the picture on the identification card;

- A report that the signature appearing on an identification card looks different than a signature on the application or other document;
- There is a discrepancy between what a person says and what is on his or her identification card;
- Information on the identification card contradicts personal information obtained from other official sources;
- Fictitious address or invalid phone number is provided by the presenter of this information;
- An applicant refuses to provide required personal information;
- Unusual Insurance Policy or Contract Activity including, but not limited to, quick cancellation, frequent address and account changes, and unexplained loan activity; and
- Mutual Trust's discovery that the security of certain personal information in our possession was recently breached.

Upon identifying the presence of any of the above indicators, Mutual Trust will conduct a thorough investigation in an attempt to rule out identity fraud as the reason for the indicator. If, upon concluding its investigation Mutual Trust cannot rule out identity fraud as the cause of an indicator, it will take the appropriate steps to notify all necessary parties, including, but not limited to, government entities, as required by law.

U.S. Life business being administered by Pan-American Life Insurance Company is monitored via Pan-American's Bridger Administrative System. (Although, Pan-American is in the process of changing its transactional administrative system to FISERV). Pan-American personnel reviewing these alerts created by their administrative system will immediately advise Mutual Trust's AML Compliance Officer of any suspected money laundering activity identified by any specific alert. Furthermore, a monthly summary report which summarizes all alerts reviewed during the prior month is provided to the Mutual Trust Compliance Officer for his review.

C. Procedures to Prevent and Mitigate Elder Financial Exploitation: Red Flags

FinCEN issued an Advisory Memorandum dated February 22, 2011 requesting the assistance of financial institutions in the identifying cases of elder financial exploitation. FinCEN recognizes that financial institutions are often quick to suspect elder financial exploitation due to the nature of the relationship it maintains with its clients. While it is clear that this advisory is greatly based on the appreciation for bank personnel familiarity with their elderly customers, there are other scenarios which may also be common to life insurance companies and reflective of elder financial exploitation. In fact, FinCEN has asked financial institutions to take advantage of the processes already in place so as to identify money laundering activity to also assist in the war against those committing elder financial exploitation by filing a SARs Report whenever financial institutions identify these types of crimes against the elderly. Mutual Trust relies on the following indicators in its attempts to identify situations where elder financial exploitation is being committed:

- A caregiver or another individual shows excessive interest in the elder's finances, does not allow the elder to speak for himself, or is reluctant to leave the elder's side during conversations;
- The elder shows an unusual degree of fear or submissiveness toward a caregiver;
- Frequent large withdrawals made from the policy;
- Taking action on a policy without regard to penalties;
- Inability to speak directly with an elder;
- A new caretaker suddenly begins conducting financial transactions on behalf of the elder without proper documentation;
- The suspicious nature surrounding the change of a power of attorney; and
- The elderly customer appears to lack knowledge about his or her financial status or insurance situation.

Mutual Trust utilizes its contact with its clients along with adopted AML technological processes such as Patriot Manager, to identify the presence of any of the above indicators. When these cases arise, Mutual Trust will conduct an investigation into the facts triggering the indicator. If, upon concluding its investigation Mutual Trust believes that it has uncovered a case of Elder Financial Exploitation, it will take the appropriate steps to notify all necessary parties, including, but not limited to, filing a Suspicious Activity Report (SAR).

D. Marijuana-Related Businesses

The Controlled Substances Act makes it illegal under federal law to manufacture, distribute, or dispense marijuana. Many states and the District of Columbia have legalized certain marijuana-related activities. U.S Department of Justice Attorney General James Cole issued a memorandum emphasizing that enforcement efforts should be applied to anyone or anything that interferes with any of the following priorities:

- Preventing the distribution of marijuana to minors;
- Preventing revenue from marijuana sales to criminal enterprises;
- Preventing the diversion of marijuana from states where it is legal to states where it is illegal;
- Preventing state-authorized marijuana activity from being used as a pretext illegal drug trafficking;
- Preventing violence and the use of firearms in the cultivation and distribution of marijuana;
- Preventing drugged driving and other adverse public health consequences stemming from marijuana use;
- Preventing the growth of marijuana on public lands along with any associated dangers; and
- Preventing marijuana possession on federal property.

FINCEN provided written guidance which clarifies how financial institutions can provide services to marijuana-related businesses with their BSA obligations. In recognition of FINCEN's written guidance and concerns relating to this issue, Mutual Trust will only consider accepting applications from anyone associated with a marijuana-related business if the proposed purchase of insurance is to address a personal need as opposed to a business need.

Mutual Trust will file the appropriate SAR if it becomes aware, suspects, or has reason to suspect that a transaction conducted or attempted by, at, or through Mutual Trust: i) involves funds or attempts to involve funds derived from illegal activity; ii) is designed to evade regulations created under the BSA, or iii) lacks an apparent lawful purpose.

If Mutual Trust should discover that it is doing business with a marijuana-related business but its business does not implicate one of the Cole Memo priorities or violate state law, it will file a "Marijuana Limited" SAR. However, upon conducting its due diligence, if Mutual Trust reasonably believes that its unintended business with a marijuana-related business violates one of the Cole Memo priorities or state law, it will file a "Marijuana Priority" SAR. If Mutual Trust feels the need to terminate its relationship with a marijuana-related business in order to maintain an effective anti-money laundering compliance program, it will file a SAR and note in the narrative the basis of such termination.

Mutual Trust is vigilant to the following Red Flags for marijuana-related businesses engaged in a business that implicates a Cole Memo priority or state law;

- A customer appearing to use a state-licensed marijuana-related business as a front to launder money obtained from marijuana-related activity not allowed under state law;
- The business cannot produce evidence that it is licensed;
- The business is unable to show the legitimate source of its outside investments;
- The customer seeks to disguise its involvement in a marijuana-related business;
- Review of publicly available sources about the business, its owners or other parties reveal negative information;
- A party related to the business is or has been subject to enforcement action by state or local authorities responsible for enforcing marijuana-related laws or regulations;
- A marijuana-related business engages in international or interstate activity;
- The owner or manager of a marijuana-related business resides outside the state in which the business is located;
- The marijuana-related business is located on federal property or the marijuana sold by the business was grown on federal property;
- A marijuana-related business's proximity to a school is not compliant with state law; and

- A marijuana-related business is purporting to be a "non-profit" business when it is engaged in commercial activity inconsistent with that classification or is making excessive payments to its managers or employees.

Now, in reality, Mutual Trust takes the position that every application must comply with Underwriting Standards and over-all Corporate Policies before it will consider issuing one of its insurance products. Due to the fact that marijuana-related businesses inherently possess certain constraints that make them less likely to comply with these standards and policies (i.e. their inability to secure checking accounts), it would be highly unlikely that Mutual Trust would unintentionally service this type of clientele.

E. Underwriting Compliance

Mutual Trust shall establish and follow procedures intended to assure that the writing of policies will be in compliance with U.S. laws. In particular, Mutual Trust shall determine that no Specially Designated National or citizen of a Sanctioned Country shall be issued a policy. In fact, every name on an application that is entered into our system is automatically OFAC checked prior to a policy being issued. This is achieved when Patriot Manager conducts an OFAC check against every name entered into the system. No policy will be issued if any name associated with an application matches a name on the OFAC list.

Furthermore, Mutual Trust's New Business Department immediately notifies the Underwriting Department if a new application is submitted in which the owner is from a foreign country. An Underwriting Representative then checks the country named on the application against the Federal Regulatory Guidelines. Mutual Trust strictly complies with these guidelines in deciding which countries Mutual Trust will do business with before it sells any product. Mutual Trust utilizes a software tool sold by its reinsurer, RGA, to access the Federal Regulatory Guidelines. The application will be promptly rejected if the owner is from a country it should not be doing business in as outlined within the Federal Regulatory Guidelines.

Mutual Trust also conducts OFAC checks before a policy is being reinstated or any addition is being made to a policy such as an increased amount of coverage or the addition of a policy rider. This is conducted via Patriot Manager.

F. Receipt of Premium Compliance

Mutual Trust shall establish and follow procedures with respect to receipt of premiums or other monies to assure compliance with U.S. laws. As a primary measure, Mutual Trust never accepts cash or currency. In addition, it is Mutual Trust 's standard policy to prohibit the receipt of cash equivalents such as money orders, cashiers checks, agency checks, or agency trust checks. This will generally prevent money laundering attempts via the utilization of a policy's free look period. However, there are occasions where our customers request that we accept a money order or cashiers check. This most often occurs when they claim not to have a personal checking account. When this arises

with new business, the Compliance Officer is consulted. Upon review of the transaction as a whole, the Compliance Officer will decide whether to make an exception to its policy prohibiting cash equivalents. If an exception is made, Mutual Trust will document the reason for the exception and encourage the applicant to secure a personal checking account to make future premium payments. When Mutual Trust receives a cash equivalent as a renewal premium payment, the Payments and Benefits Manager will approve the payment if it is within guidelines previously approved by the Compliance Officer. Of course, the risk of money laundering attempts via use of the free look period is not present here.

In the event cash is inadvertently accepted, the following steps must be followed:

- Immediately provide the cash to the Treasury Vice President;
- The Treasury Vice President shall be responsible for counting the cash. Two persons must be present to verify the amount;
- Immediately thereafter, the cash must be taken to Mutual Trust's bank for credit to the account maintained for the benefit of customers, or if no such account is available or if this approach is not feasible, obtain a cashier's check or money order made payable to a bank with which Mutual Trust has an account;
- Notify the Compliance Director promptly thereafter; and
- The Treasury Vice President shall be responsible for filing Form 4789 (Currency Transaction Report) with the Internal Revenue Service by the fifteenth (15^{th}) calendar day after receipt for cash in excess of $10,000 for any one person on any one day.

It should be noted that PALIC has much stricter requirements pertaining to its routine "Know Your Customer" investigations due its decision to enforce requirements on U.S. business normally reserved for international business.

G. Policy Change Compliance

Every policy issued by Mutual Trust provides certain ownership rights to the owner of the policy. As a part of these rights, an owner could elect to change ownership or his or her beneficiary. In recognition of this possibility, Mutual Trust's automated Patriot Manager Software System performs OFAC verification on every new owner. This action obviously eliminates any attempts to circumvent the OFAC protections put in place at the time an application is originally received and processed.

H. Claim Payment Compliance

Mutual Trust shall include wording in its claim payment and surrender checklists and approval forms, as necessary, to assure compliance with U.S. laws. An OFAC check is conducted automatically via Patriot Manager on every designated beneficiary before payment of any claim. The Compliance Officer should be informed immediately of any potential matches.

I. Outgoing Checks

Mutual Trust‘s normal business operations call for it to routinely make payments to individuals. Mutual Trust makes these payments with checks. There are a variety of reasons that can trigger Mutual Trust’s issuance of checks to individuals. For example, they include situations where Mutual Trust eceives a payment accompanied by an incomplete application, the receipt of applications that are subsequently declined, and Mutual Trust’s receipt of premium overpayments. In all of these scenarios, Mutual Trust must reimburse the payer a certain amount of money. However, prior to doing so, Mutual Trust‘s Patriot Manager Software System runs an OFAC check on the individual to be paid, including vendors, so as to assure itself that the transaction is not a veiled attempt to launder money. In addition, Mutual Trust’s Patriot Manager Software System routinely conducts an OFAC check on the recipients of Policy Loans, Withdrawals and Surrenders. Finally, the transactions are always reviewed manually for unusual activity.

Mutual Trust has also adopted GIACT, which is a vendor that confirms the authenticity of reported bank accounts. It is thru this service that Mutual Trust can confirm that a bank account belongs to a policyholder or beneficiary prior to depositing funds into that account. This process greatly reduces the risk of fraud.

J. Licensed Producers

Mutual Trust conducts a thorough background check on any new producer prior to contracting the producer. As a part of the background check conducted, Mutual Trust’s Contract and Licensing Department secures OFAC reports on all new producers. It should also be noted that Mutual Trust would be automatically notified by the appropriate State Insurance Department if any subsequent illegal activity caused the producer to lose his or her license. Furthermore, producers must routinely show evidence of a renewed producer’s license prior to its expiration date.

K. Action Taken During OFAC Screening

If the Compliance Officer identifies an individual as being on the OFAC List comprised of suspicious individuals, the Compliance Officer will take all reasonable steps to freeze any and all funds associated with his or her policy or contract. The Compliance Officer will maintain records of all actions taken. The Compliance Officer will await further instruction from the government official responsible for investigating the matter before taking any additional action on the funds frozen. Blocked and frozen accounts will be reported annually to OFAC, no later than September 30th.

L. Policy Terms

Each new policy developed by Mutual Trust shall contain all necessary wording, as required by law, concerning prohibitions against any activities which may be deemed to impede federal anti-money laundering initiatives or concerning coverage limitations,

including territorial exclusions, as necessary. Fraud language is also incorporated into applications and policies, as required.

M. Compliance Training

All full-time, hired employees, temporary employees and independent agents shall receive anti-money laundering training with respect to compliance with U.S. laws and regulations, as part of their overall training. New employees are required to receive compliance training within the first 30 days of employment. All subsequent compliance training for employees shall be provided on an annual basis. All new agents shall be required to receive compliance training before the company will issue a policy sold by him or her. The company will consider agents to have complied with this requirement if he or she received compliance training, within the last year, from a company approved educational provider. Approved providers include LIMRA, LOMA, RegEd, Quest, Broker/Dealer and FINRA AML courses, along with any NASD AML approved course. Subsequent to receiving initial AML Training, all agents are required to receive AML Training, biennially, prior to the date that he or she took their previous AML Training Course. The company sanctioned course will be provided by LIMRA.

N. Suspicious Activity Reporting and Compliance

All insurance companies are required to file Suspicious Activity Reports ("SARs") pursuant to Section 356 of the USA PATRIOT Act. Suspicious activity can occur either at the outset of the client relationship or long after the relationship has been initiated. When warranted, the Compliance Director with the approval of the firm's General Counsel, will ensure SARs are filed. If suspicious activity is identified, the matter must be immediately reported to the Compliance Director. The following Red Flag Guidelines setting forth potential indicators of suspicious activities shall be used to identify such activities:

Red Flag Guideline:

- The purchase of the Mutual Trust product appears to be inconsistent with the customer's needs;
- The customer exhibits unusual concern about the company's compliance with government reporting requirements and the company's anti-money laundering policies, particularly regarding his or her identity, type of business and assets, or is reluctant or refuses to reveal any information concerning business activities, or furnishes unusual or suspect identification or business documents;
- The information provided by the customer that identifies a legitimate source of funds is false, misleading, or substantially incorrect;
- Upon request, the customer refuses to identify or fails to indicate any legitimate source for his or her funds or other assets;

- The customer (or a person publicly associated with the customer) has a questionable background or is the subject of news reports indicating possible criminal, civil, or regulatory violations;
- The customer exhibits a lack of concern regarding risks, commissions, or other transaction costs;
- The customer appears to be acting as an agent for an undisclosed party but declines or is reluctant, without any apparent or obvious reason, to provide information or is otherwise evasive regarding that party;
- The customer has difficulty describing the nature of his or her business or lacks general knowledge of his or her industry;
- The customer attempts to make frequent or large deposits of currency that cannot be explained via a company product or concept, insists on dealing only in cash equivalents, or asks for exemptions from the company's policies relating to the deposit of cash or cash equivalents;
- For no apparent reason, the customer has multiple accounts under a single name or multiple names;
- The customer is from, or has accounts in, a country identified as a noncooperative country or territory;
- The customer's account has unexplained or sudden extensive wire activity, especially in accounts that had little or no previous activity;
- The customer's account has a large number of wire transfers to unrelated third parties inconsistent with the customer's legitimate business purpose;
- The customer's account has wire transfers that have no apparent business purpose to or from a country identified as a money laundering risk or a bank secrecy haven;
- The customer makes a funds deposit followed by an immediate request that the money be wired out or transferred to a third party, or to another firm, without any apparent business purpose;
- The customer deposits funds for the purpose of purchasing a product that produces long term benefits followed shortly thereafter by a request to liquidate the position and transfer of the proceeds out of the account;
- The customer requests that a transaction be processed to avoid the company's normal documentation requirements;
- The customer maintains multiple accounts, or maintains accounts in the names of family members or corporate entities, for no apparent purpose;
- 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;
- The transfer of the benefit of an insurance product to an apparently unrelated third party;

- Little or no concern by a customer for the investment performance of an insurance product, but much concern about the early termination features of the product; and
- The reluctance by a customer to provide identifying information when purchasing an insurance product or the providing of minimal or seemingly fictitious information.

O. FinCEN Requests under PATRIOT Act Section 314

We will respond, within 14 days, to a Financial Crimes Enforcement Network (FinCEN) request about accounts or transactions by immediately searching our records to determine whether we maintain or have maintained any account for, or have engaged in any transaction with, each individual, entity, or organization named in FinCEN's request. Upon receiving an information request, we will designate our Compliance Officer or his designee will serve as the point of contact regarding the request and to receive similar requests in the future. If we find a match, we will report directly to FinCEN the identity of the specified individual or organization, the account number, all identifying information provided by the account holder when the account was established, and the date and type of transaction. This report will be sent to FinCEN by completing FinCEN's subject information form. This form will be sent to FinCEN by electronic mail at patriot@fincen.treas.gov, by calling the Financial Institutions Hotline (1-866-556-3974), or by any other means that FinCEN specifies.

If we search our records and do not uncover a matching account or transaction, then we will not reply to a 314(a) request. We will not disclose the fact that FinCEN has requested or obtained information from us, except to the extent necessary to comply with the information request. We will maintain procedures to protect the security and confidentiality of requests from FinCEN, such as those established to satisfy the requirements of Section 501 of the Gramm-Leach-Bliley Act.

P. Sharing Information with Other Financial Institutions

Whenever the appropriate situation should arise, we will share information about those suspected of terrorism and money laundering with other financial institutions for the purposes of identifying and reporting activities that may involve terrorist acts or money laundering activities. We will file with FinCEN an initial notice before any sharing occurs and annual notices afterwards. We will use the notice form found at www.fincen.gov. We will employ strict procedures both to ensure that only relevant information is shared and to protect the security and confidentiality of this information, including segregating it from the firm's other books and records.

Mutual Trust routinely communicates with the AML Compliance Officer of Pan-American Life Insurance Company and their associated AML Officials. The purpose for these communications is so that both companies remain in tune and consistent with the culture and philosophy of the other. In order to achieve this mutual objective, the companies routinely share information regarding new AML legislative requirements.

Finally, as permitted by law, information relating to suspected money laundering activity for any U.S. individual life insurance business being administered by Pan-American Life Insurance Company shall be immediately reported to the Mutual Trust AML Compliance Officer. Furthermore, as permitted by law, Mutual Trust shall immediately notify Pan-American Life Insurance Company of any suspected money laundering activity it identifies.

Q. Record Keeping

1. SAR Maintenance and Confidentiality

We will hold SARs and any supporting documentation confidential. We will not inform anyone outside of a law enforcement or regulatory agency or securities regulator about a SAR. We will deny any subpoena requests for SARs or SAR information and immediately inform FinCEN of any such subpoena we receive. We will segregate SAR filings and copies of supporting documentation from other firm books and records to avoid disclosing SAR filings. Our Deputy General Counsel will handle all subpoenas or other requests for SARs.

2. Responsibility for Records and SAR Filing

The Deputy General Counsel will be responsible for ensuring that records are maintained properly and that SARs are filed as required. All SARs Reports will be filed within 30 days.

3. Records Required

As part of this Compliance Plan, we will create and maintain SARs, CTRs, and relevant documentation as well as any records related to customers listed on the OFAC list. We will maintain SARs and their accompanying documentation for at least five years. Other documents will be kept according to existing BSA and other record keeping requirements, including certain SEC rules that require six-year retention.

V. RESPONSIBLE OFFICIAL

The Compliance Officer is the individual with overall responsibility for day-to-day implementation of this Compliance Plan. John P. Seneczko, telephone number 630-684-5481, email address seneczkoj@mutualtrust.com is designated as the Compliance Officer with the authority to implement the procedures described in this Compliance Plan. Geri Gaughan, President and Chief Operating Officer, may also be contacted at 630-684-5430, email address gaughang@mutualtrust.com.

In addition to duties described elsewhere in this Compliance Plan, the Compliance Officer has the responsibilities set forth below.

A. Risk Assessment

The Compliance Officer is responsible for assessing the associated money laundering risk associated with every Mutual Trust product and the processes in place to market every product. The Compliance Officer shall require all affected personnel to take the steps necessary to reduce money laundering risks to a reasonable and manageable amount. The company conducts a formal risk assessment annually.

B. Communication of Information to Employees

The Compliance Officer shall make available to all employees the company's Compliance Plan.

C. Training

The Compliance Officer shall provide the means for employees to take Anti-Money Laundering Training. This on-line training program is sponsored by LIMRA, a third party vendor widely recognized as a thorough educational guide that addresses pertinent Anti-Money Laundering issues affecting the insurance industry. This on-line training program for Mutual Trust employees is not optional and in fact, is a mandated requirement for all affected Mutual Trust employees. New employees are required to complete AML training within 30 days of hire. The Compliance Officer shall verify and monitor that all employees have received annual AML training as set forth in this Compliance Plan.

Also, advancements in technology will continue to be incorporated into the corporate-wide program to assist in maintaining Anti-Money Laundering Compliance. Mutual Trust Insurance remains interested in any technological advancement that will assist the company in its efforts to make sure that it remains aware of suspicious activity so that it may conduct the appropriate investigation into it. Furthermore, any technological improvement adopted by the company should be compatible to and practical for the business Mutual Trust Insurance produces.

In addition, as issues arise, the Compliance Officer shall routinely reinforce to each person involved in the receipt of policy premiums that as a rule, Mutual Trust does not accept cash. Also, money orders, cashiers checks, agency checks, agency trust checks, or the equivalents to cash or currency, are prohibited unless a reasonable justification for acceptance can be established.

D. Reporting

The Compliance Officer shall monitor activities under this compliance program and shall submit annual reports on completion of required activities to General Counsel and Internal Audit no later than May 1 of each year.

E. Ongoing Review of Compliance Plan

The Compliance Officer, at least annually, shall conduct a review of the compliance program and the procedures developed and implemented pursuant to this Compliance Plan. The Compliance Director shall suggest revisions to the compliance program to reflect changes in the law and regulations as well as other changes, such as those resulting from advances in technology.

VI. COMPLIANCE MONITORING

A. Independent Audits

The testing of the AML program will be performed every two years by the Internal Audit Department, who are personnel of our firm and report directly to the Audit Committee, all of whom are independent Board of Director members. The Internal Audit Department does not perform the AML functions being tested nor do they report to any such persons. Their qualifications include a working knowledge of applicable requirements under the anti-money laundering regulations. Independent testing will be performed more frequently if circumstances warrant.

In general the independent testing is initiated as part of the requirement that an insurance company provide for independent testing of the program on a periodic basis to ensure that it complies with the requirement of the rule and that the program functions as designed. The objective of the audit is to determine whether the insurance company controls over the Anti-Money Laundering Program as set forth under the USA PATRIOT Act and Federal Register – Vol. 70, No. 212 / Department of the Treasury 31 CFR Part 103 (RIN 1506-AA70) provide reasonable assurance that program objectives may be achieved.

The Internal Audit Department is responsible for designing and executing the independent audit program supporting Mutual Trust Life Insurance Company's anti-money laundering program. In general, this independent audit includes, but is not limited to, the examination of the policies and procedures stated in the documented policy; evaluating the adequacy and reasonableness of the control environment; observations and interviews with selected aspects of the program, including SAR reporting; and testing the operation of the control environment through certain sample selections.

B. Automated Daily Reporting System

Mutual Trust shall utilize Patriot Manager as a means of generating routine and daily computerized reports so as to better monitor that it is taking affirmative action to investigate and handle potential suspicious policy activity and comply with all legally mandated reporting. This system will monitor account activity for unusual patterns or types of transactions, taking into account risk factors along with common customer activities and motivations. Automated reports are automatically retained concerning the results of the individual analysis conducted on such transactions. The AML Compliance Person or his or her designee will be responsible for this monitoring, will review any activity that our monitoring system detects, will determine whether any additional steps

are required, will document when and how this monitoring is carried out, and will report suspicious activities to the appropriate authorities.

C. Manual Monitoring

Mutual Trust personnel that are responsible for handling routine customer transactions are also personally responsible for remaining vigilant for suspicious money laundering activity. Red Flags for such activity are outlined in item IV.N of this document. Mutual Trust personnel are instructed to document any identified suspicious activity and alert their managers, who, in turn, are responsible for notifying the AML Compliance Officer. Upon receiving a report about a compliance matter, the Compliance Officer shall take immediate and decisive action as described in Section E below. In addition, the Compliance Officer shall maintain a record of all reports from employees, including the nature of any internal review and its results.

It is also Mutual Trust's general policy to prohibit cash and cash equivalents. However, situations will occasionally arise where the spirit of fair dealing dictates Mutual Trust make an exception to this general policy and accept a cash equivalent. However, this will only occur with approval from the AML Compliance Officer and a definitive determination is made that the payment is not indicative of money laundering activity or any other inappropriate behavior. If an exception is made, the file is documented accordingly to reflect the reason the exception is made.

There are occasions, however, when a cash equivalent is received by Mutual Trust's lockbox procedure for receipt of payments. When this occurs, the bank will refer the cash equivalent payment to Mutual Trust for further review if it meets certain criteria so as to mitigate against the potential for money laundering activity. The Payments and Benefits Manager receives a weekly report of such lockbox cash equivalents received. A Representative reviews these payments. If the payment is suspicious in nature, the AML Compliance Officer is notified immediately. If the payment appears justified due to the fact that it falls within certain parameters previously agreed to by the Compliance Officer, the reason it is justified is documented on the report. The AML Compliance Officer monitors these reports and subsequent reviews by the Project Coordinator on a monthly basis.

D. AML Committee

In 2008, Mutual Trust instituted an Anti-Money Laundering (AML) Committee Charter which gave rise to the creation of Mutual Trust's AML Committee. The AML Committee is charged with the responsibility of creating an effective AML program which encompasses processes put in place to help prevent and identify money laundering activity along with complying with all applicable Federal Laws and Regulations. Every AML Committee meeting includes an OFAC Report as a means of monitoring the continual comparison of names within our systems to those on the OFAC Watch List. The AML Committee is comprised of the AML Compliance Officer, the Internal Audit Officer, the Contracts and Licensing Manager, the Underwriting Manager, the Law

Department Paralegal and the Director of Policy Owner Services. It meets on a quarterly basis to discuss these issues and committee reports are provided to the company's Best Practices Committee.

E. Required Action

The Compliance Officer shall take the following action based on information obtained as a result of a compliance audit:

- Take appropriate steps to secure or preserve documents or other evidence relevant to the internal review;
- Work with Internal Audit to conduct an internal review of the compliance matter;
- Maintain a complete record with respect to the internal review including, but not limited to: (1) a description of the process, including methodologies used in connection with the process; (2) copies of key documents; and (3) a log of the employees interviewed and the documents reviewed; and
- Discuss the results of the internal review with Internal Audit and recommend action to be taken. Also recommend any changes in internal controls, policy modifications and any other appropriate remedial steps as required.

VII. DISCIPLINARY ACTION

Mutual Trust personnel policies require employees to follow the company's written instructions and procedures. Consistent with these policies, Mutual Trust may impose disciplinary measures for actions not in compliance with this Compliance Plan.