

Bankers Life Insurance Company

ANTI-MONEY LAUNDERING COMPLIANCE POLICY

Policy Statement and Principles

It is the policy of Bankers Life Insurance Company (“BLIC”) to prohibit and actively pursue the prevention of money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities. BLIC is committed to Anti-Money Laundering (“AML”) compliance in accordance with the Bank Secrecy Act, as amended by the USA PATRIOT Act of 2001 (the “Act”) and 31 CFR § 103.137 and other applicable law and requires its officers, employees and appointed producers to adhere to these standards in preventing the use of its products and services for money laundering purposes. Failure by BLIC to comply with the Act could result in severe regulatory sanctions, possible fines and criminal penalties and damage to the BLIC’s business reputation.

To ensure that the foregoing general policy statement is carried out, and to ensure compliance with the Act, the BLIC Board of Directors has established and approved this AML policy (“Policy”).

Scope of Policy

The Policy applies to all BLIC officers, employees, and appointed producers who deal, handle, service or promote Covered Products (as this term is defined below).

Definition of Money Laundering

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 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.

AML Compliance Officer and Coordinator

BLIC designated its Deputy General Counsel as the company's AML Compliance Officer ("the AMLCO").

The AMLCO is responsible for:

- Implementing the Policy
- Amending the Policy as necessary
- Educating and training those expected to adhere to the Policy

The AMLCO should be given access to all departments and documentation that may be necessary to carry out the foregoing responsibilities. The AMLCO should have the authority to implement corrective action upon discovering actual or possible violations. It is the policy of BLIC to have all suspicious activity reported to the AMLCO for review and determine if filing a Suspicious Activity Report is warranted.

Covered Products

In the insurance context, the final regulations define "Covered Products" to include: (1) permanent life insurance policies, other than group life insurance; (2) annuity contracts, other than group annuity contracts; or (3) any other insurance products with features of cash value or investment. BLIC currently offers fixed and variable annuities, which meet the definition of a Covered Products.

Risk Assessment

BLIC conducted an assessment of the risk of exposure to money laundering within BLIC's Covered Products. This assessment was completed with consideration to customer types that have been deemed by the federal regulatory agencies to pose a higher risk of exposure to money laundering concerns. The assessment rates customers considering a number of factors including: reputation, geographical location/local AML regulations, business type, entity type/structure, product type and liquidity of assets. Customers deemed to be high-risk should be subject to enhanced due diligence at account opening, stringent transaction monitoring throughout their relationship with BLIC. Customer risk assessments should be reevaluated upon any material change to a customer's information.

Although BLIC's Covered Products may be purchased to launder funds and hide criminal activity, by not accepting cash payments (i.e. money orders, cashier's check) or offshore funds, the risk of criminal activity is significantly reduced.

Customer Identification Program

BLIC adopted a customer identification program, which enables BLIC to form a reasonable belief that it knows the true identity of each customer. BLIC, through its appointed producers, will provide notice to its customers that it will:

- collect certain minimum customer identification information from each customer,
- record such information and the verification methods and results, and
- compare customer identification information with the Office of Foreign Asset Control (“OFAC”).

Notice to Customers

BLIC, through its appointed producers, will provide notice to customers that it is requesting information from them to verify their identities, as required by applicable law. The following notice will be used:

To help fight the funding of terrorism and money-laundering activities, our company’s policy is to obtain, verify and record information that may identify a person or persons who engage in certain transactions with or through Bankers Life Insurance Company. This means that we will verify your name, residential or street address, date of birth and social security number or other tax identification number on the application. We may also ask to see a driver’s license or other identifying documents from you.

Required Customer Information

The following information will be collected, by BLIC’s appointed producers, for all new insurance and annuity applications:

- Name,
- Date of birth,
- Address,
- Identification number, which will be a social security number (“SSN”) or taxpayer identification number (“TIN”) for U.S. persons or entities,
- Photo identification (drivers license or other comparable source) or, for non-U.S. persons or entities, one or more of the following:
 - Passport number and country of issuance,
 - Alien identification card number or;
 - Number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or other similar safeguard.
- Source of funds
- References

Verifying Information

BLIC’s appointed producers should not attempt to determine whether the document that the customer has provided to them for identification has been validly issued. For verification purposes, BLIC’s appointed producers shall rely on a government-issued identification to establish a customer’s identity. However, BLIC’s appointed producers will

be instructed to analyze the information provided to determine if there are any logical inconsistencies in the information obtained.

BLIC will document its verification, including all identifying information provided by the customer, the methods used and results of the verification, including but not limited to sign-off by the appointed producer of matching photo identification. BLIC will maintain all records used to identify and verify each customer's identification for five years after the date the account is closed.

If BLIC is unable to form a reasonable belief that it knows the true identity of a customer within 90 days of an application, the application will be denied. During that 90 days such an applicant will be subject to increased due diligence.

Customers Who Refuse To Provide Information

If a customer either refuses to provide the information described above when requested, or appears to have intentionally provided misleading information, the appointed producer shall immediately notify the AMLCO and decline the application.

Checking the Office of Foreign Assets Control ("OFAC") List

For all (1) new applications received and on an ongoing basis, (2) disbursements (3) new producers appointed or (4) new employees, BLIC will check to ensure that a person or entity does not appear on the Treasury's OFAC "Specifically Designated Nationals and Blocked Persons" List (SDN List) and is not from, or engaging in transactions with people or entities from, embargoed countries and regions listed on the OFAC Web Site. BLIC contracted with ChoicePoint's Bridger Systems to ensure speed and accuracy in the checks. BLIC will also review existing policyholders, appointed producers and employees against these lists on a weekly basis.

In the event of a match to the SDN List or other OFAC List, BLIC will conduct a review of the circumstances where such match has been identified. If BLIC is unable to confirm that the match is a false positive, the AMLCO will be immediately notified.

Monitoring and Reporting

While BLIC does not currently accept cash or monetary instruments (i.e. money orders, cashier's checks) from its customers, BLIC will comply with currency transaction reporting requirements ("CTR") in the event this policy changes. BLIC will report to the Internal Revenue Service, in compliance with I.R.C. § 6050I, each deposit, withdrawal, and exchange of cash that exceeds \$10,000 in any one transaction or any two or more related transactions that occur within a 24-hour period. Cash includes currency, such as coin or paper money of the United States or a foreign country, and monetary instruments, including a cashier's check, money order, bank draft or traveler's check, which do not exceed \$10,000 in value.

In addition, BLIC will monitor for suspicious activity. There are signs of suspicious activity that suggest money laundering. These are commonly referred to as "red flags." If a

red flag is detected, additional due diligence will be performed before proceeding with the transaction. If a reasonable explanation is not determined, the suspicious activity shall be reported to the AMLCO. No employee, nor appointed producer, may inform or “tip-off” the customer that BLIC has detected potential suspicious activity.

Examples of red flags are:

- The customer exhibits unusual concern regarding the Policy and government reporting requirements, particularly with respect to 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 customer wishes to engage in transactions that lack business sense or apparent investment strategy, or are inconsistent with the customer’s stated business strategy.
- The information provided by the customer that identifies a legitimate source for 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 and other assets.
- The customer is using funds from an offshore account.
- 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 principal, but declines or is reluctant, without legitimate commercial reasons, to provide information or is otherwise evasive regarding that person or entity.
- 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, insists on dealing only in cash equivalents, or asks for exemptions from the firm's policies relating to the deposit of cash and cash equivalents.
- 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.

- For no apparent reason, the customer has multiple accounts under a single name or multiple names, with a large number of inter-account or third-party transfers.
- The customer is from, or has accounts in, a country identified as a non-cooperative country or territory by the Financial Action Task Force.
- 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 shows numerous currency or cashiers check transactions aggregating to significant sums.
- 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 money laundering risk or a bank secrecy haven.
- The customer's account indicates large or frequent wire transfers, immediately withdrawn by check or debit card without any apparent business purpose.
- 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 makes a funds deposit for the purpose of purchasing a long-term investment followed shortly thereafter by a request to liquidate the position and transfer of the proceeds out of the account.
- The customer engages in excessive journal entries between unrelated accounts without any apparent business purpose.
- The customer requests that a transaction be processed in such a manner to avoid the firm's normal documentation requirements.
- The customer, for no apparent reason or in conjunction with other red flags, engages in transactions involving certain types of securities, such as penny stocks, Regulation S ("Reg S") stocks, and bearer bonds, which although legitimate, have been used in connection with fraudulent schemes and money laundering activity. (Such transactions may warrant further due diligence to ensure the legitimacy of the customer's activity.)
- The customer's account shows an unexplained high level of account activity with very low levels of securities transactions.
- Attempt to borrow maximum cash value of a single premium policy soon after purchase.

- Any other activity that indicates to you that a person or persons may be attempting to launder money.
- If the appointed producer:
 - Exhibits a dramatic or unexpected increase in sales (particularly of single premium contracts)
 - Has consistently high activity in single premium contracts in excess of company averages
 - Exhibits a sudden change in lifestyle
 - Requests client documentation be delivered to the agent

Investigation

Upon notification to the AMLCO of a match to the OFAC SDN List or possible suspicious activity, an investigation will be commenced to determine if a report should be made to appropriate law enforcement or regulatory agencies. The AMLCO is responsible for any notice or filing with law enforcement or regulatory agency.

If the AMLCO determines that a Suspicious Activity Report (“SAR”) should be filed, the AMLCO will ensure that the SAR is completed and filed within thirty (30) days after BLIC identified the activity as suspicious pursuant to 12 CFR Part 353. The AMLCO will maintain a filing system for all SARs filed. The AMLCO shall promptly notify BLIC’s Board of Directors or a committee thereof, at the next scheduled Board meeting regarding recent SAR activity.

Investigation results should not be disclosed or discussed with anyone other than those who have a legitimate need to know. Under no circumstances shall any officer, employee or appointed agent disclose or discuss any AML concern, investigation, notice or SAR filing with the person or persons subject of such, or any other person, including members of the officer’s, employee’s or appointed agent’s family. Disclosure of such is strictly prohibited by the Act.

Recordkeeping

The AMLCO will be responsible to ensure that AML records are maintained properly and that SARs and Blocked Property Reports are filed as required. BLIC will maintain AML records for at least five years. The five-year retention period will be applied for five years after the policy or contract is surrendered, lapsed, terminated by death, or closed for any reason.

Training

To ensure awareness of requirements under the Act, BLIC contracted with LIMRA to provide general AML training to its officers, employees and appointed producers. Generally, all training should include, at a minimum: how to identify red flags and signs of money laundering, what roles the officers, employees and appointed producers have in the BLIC compliance efforts and how to perform such duties and responsibilities, what to do once a red flag or suspicious activity is detected, BLIC record retention policy, and the disciplinary consequences for non-compliance with the Act and this Policy.

Training will be conducted on an annual basis. The AMLCO will determine the ongoing training requirements and ensure written procedures are updated to reflect any changes required in such training. BLIC will maintain records to document that training occurred.

In addition, BLIC will provide enhanced training in accordance with the procedures developed in each department for officers and employees reasonably expected to handle money, requests, or processing, which may bring them into contact with the information designated above.

A licensed producer who completes AML training in compliance with the Act may be appointed by BLIC. The AMLCO may rely upon such training as satisfying the Policy's training requirements if the training has been completed through LIMRA, or has been certified by the AMLCO or other appropriate authority of the producer's former company as in compliance with the Act.

In the event a producer receives training via a third party not subject to the AML requirements under Section 352 of the USA PATRIOT Act, BLIC's AMLCO should determine whether such training meets the requirements of the BLIC AML training program.

Disciplinary Action

Each employee whose duties involve compliance with the Act is expected to know the requirements of the Act and regulations affecting his or her job responsibilities. It shall be the affirmative duty of such employee to carry out these responsibilities at all times in a manner that complies with the requirements of the Act. Any employee failing to comply with this policy will be subject to disciplinary action, up to and including termination.

Testing of the Policy

Independent testing for compliance with the Acts shall be conducted annually by Bankers Financial Corporation's (BLIC's ultimate parent) Internal Audit Department. The Internal Audit Department shall document the scope of testing procedures performed and issue a report covering the findings of the audit. At a minimum the audit shall include: (i) an evaluation of the overall integrity and effectiveness of the AML compliance program, including policies, procedures and processes; (ii) a review of the Policy's risk assessment for reasonableness given BLIC's risk profile; (iii) appropriate suspicious activity testing,

including testing directed to insurance agents and insurance brokers, and transaction testing to verify BLIC's adherence to the Policy's reporting requirements; (iv) an evaluation of management's efforts to resolve violations and deficiencies noted in previous audits and regulatory examinations; (v) a review of staff training; (vi) an assessment of the overall process for identifying and reporting suspicious activity.

Any findings should be reported to the AMLCO and BLIC's Senior Management for appropriate action. The AMLCO is responsible for the administration, revision, interpretation, and application of this Policy