WCU FINANCIAL
ESTABLISHED IN 1877
FAITH | STRENGTH | SECURITY

Western Catholic Union
A Fraternal Benefit Society
510 Maine St, Quincy, IL 62301
217-223-9721 • Fax: 217-223-9726
www.wculife.org

WCU ANTI-MONEY LAUNDERING (AML) COMPLIANCE

1. Western Catholic Union AML Policy

It is the policy of Western Catholic Union (WCU) 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 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 could be for criminal purposes.

Our AML policies, procedures and internal controls are designed to ensure compliance with all applicable BSA regulations and FINRA rules and 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.

2. AML Compliance Officer Designation and Duties

WCU designates the Secretary-Treasurer as the Anti-Money Laundering Program Compliance Officer, with full responsibility for the WCU's AML program. The AML Compliance Officer is qualified by experience, knowledge and training. They keep in contact with legal counsel and use sources such as MIB and OFAC software to help monitor our business activity. The duties of the AML Compliance Officer includes monitoring WCU's compliance with AML obligations, overseeing communication and training for employees, and keeping all others who may be affected aware of our needs to remain in compliance. The AML Compliance Officer will also ensure that proper AML records are kept. When warranted, the AML Compliance Officer in consultation with other National Officers, legal counsel, and employees will ensure Suspicious Activity Reports (SAR-ICs) are filed.

3. Giving AML Information to Federal Law Enforcement Agencies and Other Financial Institutions

FinCEN Requests Under USA PATRIOT Act Section 314(a)

WCU will respond to a Financial Crimes Enforcement Network (FinCEN) request concerning accounts or transactions by immediately searching its 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 one person to be the point of contact regarding the request and to receive similar requests in the future.

Unless otherwise stated in FinCEN's request, we are required to search current accounts, accounts maintained by a named suspect during the preceding 12 months, and transactions conducted by or on behalf of or with a named subject during the preceding six months. If we find a match, we will report it to FinCEN via FinCEN's Web-based 314(a) Secure Information Sharing System. This form can be sent to FinCEN by electronic mail at sys314a@fincen.treas.gov, or by fax to 703-905-3660. If the search parameters differ from those mentioned above (for example, if FinCEN requests longer periods of time or limits the search to a geographic location), we will structure our search accordingly.

If we search our records and do not find a matching account or transaction, then we will not reply to the 314(a) request. We will maintain documentation that we have performed the required search.

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 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 Section 501 of the Gramm-Leach-Bliley Act with regard to the protection of customers' nonpublic information.

We will direct any questions we have about the 314(a) Request to the requesting Federal law enforcement agency as designated in the request.

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

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

Before accepting an application for membership, we will check to ensure that a benefit member does not appear on Treasury's OFAC "Specifically Designated Nationals and Blocked Persons" List (SDN List)(See the OFAC Web Site at www.treas.gov/ofac, which is also available through an automated search tool on www.nasdr.com/money.asp), or is not engaging in transactions that are prohibited by the economic sanctions and embargoes administered and enforced by OFAC. Because the OFAC Web Site is updated frequently, we will consult the list on a regular basis and subscribe to receive updates when they occur. With respect to the OFAC SDN list, we may also access that list through various software programs to ensure speed and accuracy. We also will review existing accounts against the SDN list and listings of current sanctions and embargoes when they are updated and we will document the review.

If we determine that a benefit member, or someone with or for whom the benefit member is transacting, is on the SDN List or is engaging in transactions that are prohibited by the economic sanctions and embargoes administer and enforced by OFAC, we will reject the transaction and/or block the benefit member's assets and file a blocked assets and/or rejected transaction form with OFAC. We will also call the OFAC Hotline at 1-800-540-6322.

5. Customer Identification Program

a. Required Benefit Member Information

We will collect the following information for all benefit members who open a new account: the name; date of birth (for an individual); an address, which will be a residential or business street address (for an individual), an Army Post Office ("APO") or Fleet Post Office ("FPO") number, or residential or

business street address of next of kin or another contact individual (for an individual who does not have a residential or business street address), or a principal place of business, local office or other physical location (for a person other than an individual); an identification number, which will be a taxpayer identification number (for U.S. persons) or one or more of the following: a taxpayer identification number, 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 (for non-U.S. persons).

b. Benefit Members Who Refuse to Provide Information

If a potential or existing benefit member either refuses to provide the information described above when requested, or appears to have intentionally provided misleading information, WCU will not accept the application for insurance or for an annuity and, after considering the risks involved, consider closing any existing account(s). In either case, our AML Compliance Officer will be notified so that we can determine whether we should report the situation to FinCEN on a SAR.

c. Verifying Information

Based on the risk, and to the extent reasonable and practicable, we will ensure that we have a reasonable belief that we know the true identity of our benefit members by using risk-based procedures to verify and document the accuracy of the information we get about our benefit members. We will analyze the information we obtain to determine whether the information is sufficient to form a reasonable belief that we know the true identity of the benefit member (e.g., whether the information is logical or contains inconsistencies).

We will verify benefit member identity through documentary means, non-documentary means, or both. We will use documents to verify benefit member identity when appropriate documents are available. In light of the increased instances of identity fraud, we will supplement the use of documentary evidence by using the non-documentary means described below whenever necessary. We also may use non-documentary means, if we are still uncertain about whether we know the identity of the benefit member. In verifying the information, we will consider whether the identifying information that we receive, such as the benefit member's name, street address, zip code, telephone number (if provided), date of birth, and social security number allow us to determine that we have a reasonable belief that we know the true identity of the benefit member.

Appropriate documents for verifying the identity of benefit members include, but are not limited to the following:

- Independently verifying the member's identity through the comparison of information provided by the customer with information obtained from a consumer reporting agency, public database or other source.
- For an individual, an unexpired government-issued identification evidencing nationality, residence, and bearing a photograph or similar safeguard, such as a driver's license or passport; and
- For a person other than an individual, documents showing the existence of the entity, such as certified articles of incorporation, a government-issued business license, a partnership agreement or a trust instrument.

We understand that we are not required to take steps to determine whether the document that the benefit member has provided to us for identity verification has been validly issued and that we may rely on a government-issued identification as verification of a benefit member's identity. If however, we note that the document shows some obvious form of fraud, we must consider that factor in determining whether we can form a reasonable belief that we know the benefit member's true identity.

We will use the following non-documentary methods of verifying identity:

- Contacting a benefit member;
- Independently verifying the benefit member's identity through the comparison of information provided by the benefit member with information obtained from a consumer reporting agency, public database, or other source;
- Checking references with other financial institutions; or
- Obtaining a financial statement.

We will use non-documentary methods of verification when:

1. The benefit member is unable to present an unexpired government-issued identification document with a photograph or other similar safeguard.
2. We are unfamiliar with the documents the benefit member presents for identification verification.
3. The benefit member and WCU do not have face-to-face contact; and
4. There are other circumstances that increase the risk that we will be unable to verify the true identity of the benefit member through documentary means.

We will verify the information within a reasonable time before or after the account is opened. Depending on the nature of the account and requested transactions, we may refuse to accept an application for membership and/or complete a transaction before we have verified the information, or in some instances when we need more time, we may, pending verification, restrict the types of transactions or dollar amount of transactions. If we find suspicious information that indicates possible money laundering, terrorist financing activity, or other suspicious activity, we will, after internal consultation with WCU's AML Compliance Officer, file a SAR in accordance with applicable laws and regulations.

We recognize that the risk, if we do not know the benefit member's true identity, may be heightened for certain types of insurance products, such as an annuity. We will identify benefit members that pose a heightened risk of not being properly identified.

d. Lack of Verification

When we cannot form a reasonable belief that we know the true identity of a benefit member/applicant, we will do the following: (1) not offer the product; (2) impose terms under which a benefit member may conduct transactions while we attempt to verify the benefit member's identity; (3) close an account after attempts to verify benefit member's identity fail; and (4) determine whether it is necessary to file a SAR in accordance with applicable laws and regulations.

e. Recordkeeping

We will document our verification, including all identifying information provided by a benefit member, the methods used and results of verification, and the resolution of any discrepancies identified in the verification process. We will keep records containing a description of any document that we relied on to verify a benefit member's identity, noting the type of document, any identification number contained in the document, the place of issuance, and if any, the date of issuance and expiration date. With respect to non-documentary verification, we will retain documents that describe the methods and the results of any measures we took to verify the identity of a benefit member. We

will also keep records containing a description of the resolution of each substantive discrepancy discovered when verifying the identifying information obtained. We will retain records of all identification information for five years after the account has been closed; we will retain records made about verification of the benefit member's identity for five years after the record is made.

f. Comparison with Government Provided Lists of Terrorists

At such time as we receive notice that a Federal government agency has issued a list of known or suspected terrorists, we will, within a reasonable period of time after an account is opened (or earlier, if required by another Federal law or regulation or Federal directive issued in connection with an applicable list), determine whether a benefit member appears on any such list of known or suspected terrorists or terrorist organizations issued by any Federal government agency and designated as such by Treasury in consultation with the Federal functional regulators. We will follow all Federal directives issued in connection with such lists. We will check each new application for the insured, owner and beneficiary against the known listing of suspected terrorists as listed by the Treasury Department.

g. Notice to Benefit Members

We will provide notice to benefit members that WCU is requesting information from them to verify their identities, as required by Federal law. WCU provides notice to benefit members via our Privacy Notice which is mailed annually to all members and posted on our website.

Important Information About Procedures for Opening a New Account
To help the government fight the funding of terrorism and money laundering activities, federal law requires all fraternal benefit societies to obtain, verify, and record information that identifies each person who opens an account.

What this means for you: When you open an account, we will ask for your name, address, date of birth and other information that will allow us to identify you. We may also ask to see your driver's license or other identifying documents.

6. Monitoring Accounts for Suspicious Activity

We will manually monitor a sufficient amount of account activity for unusual size, volume, pattern or type of transactions, taking into account risk factors and red flags identified below. We will look at transactions, including wire transfers, in the context of other account activity to determine if a transaction lacks financial sense or is suspicious because it is an unusual transaction or strategy for that benefit member. The AML Compliance Officer or his or her designees (any employee making payments or accepting payments on behalf of WCU) will be responsible for this monitoring, will document when and how it is carried out and will report suspicious activities to the appropriate authorities. Among the information we will use to determine whether to file a Form SAR are exception reports that include transaction size, location, type, number, and nature of the activity. We will create employee guidelines with examples of suspicious money laundering activity and lists of high-risk members whose accounts may warrant further scrutiny. Our AML Compliance Officer will conduct an appropriate investigation before a SAR is filed.

a. Red Flags

Red flags that signal possible money laundering or terrorist financing include, but are not limited to:

- The benefit member exhibits unusual concern about WCU's compliance with government

reporting requirements and our AML policies (particularly concerning his or her identity, type of business and assets), or is reluctant or furnishes unusual or suspicious identification.

- The benefit member wishes to engage in transactions that lack business sense or apparent investment strategy, or are inconsistent with the benefit member's stated needs.

- The information provided by the benefit member that identifies a legitimate source for funds is false, misleading, or substantially incorrect.

- Upon request, the benefit member refuses to identify or fails to indicate any legitimate source for his or her funds and other assets.

- The benefit member (or a person publicly associated with the benefit member) has a questionable background or is the subject of news reports indicating possible criminal, civil, or regulatory violations.

- The benefit member exhibits a lack of concern regarding risks, commissions, or other transaction costs.

- The benefit member appears to be acting as an agent for an undisclosed principal, but declines or is reluctant, without legitimate reasons, to provide information or is otherwise evasive regarding that person.

- The benefit member attempts to make frequent or large deposits of currency, insists on dealing only in cash, or asks for exceptions from WCU's policies relating to the deposit of cash.

- The benefit member 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 benefit member 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 benefit member requests that a transaction be processed to avoid WCU's normal documentation requirements.

- The benefit member maintains multiple accounts, or maintains accounts in the names of family members, for no apparent purpose.

- The benefit member's account has inflows of funds or other assets well beyond the known income or resources of the benefit member.

- The benefit member requests a transfer of funds to an unrelated third party for no apparent purpose.

- The beneficiary of the member/applicant has an unclear or no insurable interest.

- The member/applicant designates an unusual beneficiary and or assignee.

- The member enters into an unusual viatical sale.

- Any other unusual transaction.

b. Responding to Red Flags and Suspicious Activity

When a member of WCU detects any red flag he or she will investigate further under the direction of the AML Compliance Officer. This may include gathering additional information internally or from third-party sources, contacting the government, or filing a Form SAR-IC.

7. Suspicious Transactions and BSA Reporting

a. Filing a SAR

We will file SARs with FinCEN for any transactions (including deposits and transfers) conducted or attempted by, at or through WCU involving $5,000 or more of funds or assets (either individually or in the aggregate) where we know, suspect, or have reason to suspect:

1) The transaction involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity as part of a plan to violate or evade federal law or regulation or to avoid any transaction reporting requirement under federal law or regulation;
2) The transaction is designed, whether through structuring or otherwise, to evade the any requirements of the BSA regulations;
3) The transaction has no business or apparent lawful purpose or is not the sort in which the benefit member would normally be expected to engage, and after examining the background, possible purpose of the transaction and other facts, we know of no reasonable explanation for the transaction; or
4) The transaction involves the use of WCU to facilitate criminal activity.

We will not base our decision on whether to file a SAR solely on whether the transaction falls above a set threshold. We will file a SAR and notify law enforcement in situations involving violations that require immediate attention, such as terrorist financing or ongoing money laundering schemes. We will not file SARs to report violations of that do not involve money laundering or terrorism.

All SARs will be periodically reported to the senior management, with a clear reminder of the need to maintain the confidentiality of the SAR.

We will report suspicious transactions by completing a SAR, and we will collect and maintain supporting documentation as required by the BSA regulations. We will file a SAR-SF no later than 30 calendar days after the date of the initial detection of the facts that constitute a basis for filing a SAR. If no suspect is identified on the date of initial detection, we may delay filing the SAR for an additional 30 calendar days 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.

We will retain copies of any SAR filed and the original or business record equivalent of any supporting documentation for five years from the date of filing the SARSF. We will identify and maintain supporting documentation and make such information available to FinCEN, any other appropriate law enforcement agencies, or federal or state regulators, or SROs upon request.

We will not notify any person involved in the transaction that the transaction has been reported, except as permitted by the BSA regulations. We understand that anyone who is subpoenaed or required to disclose a SAR or the information contained in the SAR will, except where disclosure is requested by

FinCEN, or another appropriate law enforcement or regulatory agency, decline to produce to the SAR or to provide any information that would disclose that a SAR was prepared or filed. We will notify FinCEN of any such request and our response.

b. Currency Transaction Reports (CTR)

WCU prohibits the receipt of currency over $5,000 and has the following procedures to prevent such transactions: If it does reach our office it will be immediately returned. If we discover such transactions have occurred, we will file with FinCEN CTRs for currency transactions that exceed $10,000. Also we will treat multiple transactions involving currency as single transaction for purposes of determining whether to file a CTR if they total more than $10,000 and are made by or on behalf of the same person during any one business day. We will use the BSA E-filing System to file the supported CTR form.

8. AML Recordkeeping

a. Responsibility for Required AML Records and SAR Filing

Our AML Compliance Officer and his or her designee will be responsible to ensure that AML records are maintained properly and that SARs are filed as required.

b. SAR Maintenance and Confidentiality

We will hold SARs and any supporting documentation confidential. We will not inform anyone outside of FinCEN, a law enforcement or regulatory agency about a SAR. We will refuse any subpoena requests for SARs or for information that would disclose that a SAR has been prepared or filed and immediately notify FinCEN of any such subpoena requests we receive. We will segregate SAR filings and copies of supporting documentation from other WCU books and records to avoid disclosing SAR filings. Our AML Compliance Officer will handle all subpoenas or other requests for SARs.

c. Additional Records

We shall retain either an original or copy of each of the following:

- A record of each advice, request or instruction received or given regarding any transaction resulting (or intended to result and later canceled if such a record is normally made) in the transfer of currency or other monetary instruments, funds, checks, investment securities or credit, of more than $10,000 to or from any person, account or place outside the U.S.;
- As part of our AML program, WCU will create and maintain SAR-ICs, CTRs, and relevant documentation on benefit member identity and verification (*See* Section 5 above) and funds transfers and transmittals as well as any records related to benefit members listed on the OFAC list. We will maintain SAR-ICs and their accompanying documentation for at least five years. We will keep other documents according to existing BSA and other record-keeping requirements.

9. Training Programs

We will develop ongoing employee training under the leadership of the AML Compliance Officer and senior management. Our training will occur when an individual is either hired or transferred to an appropriate position and thereafter on at least an annual basis for current employees. It will be based

on WCU's size, its benefit member base, and its resources and be updated as necessary to reflect any new developments in the law.

Our training will include, at a minimum: (1) how to identify red flags and signs of money laundering that arise during the course of the employees' duties; (2) what to do once the risk is identified (including how, when and to whom to escalate unusual customer activity or other red flags for analysis and where appropriate, the filing of SARs); (3) what employees' roles are in WCU's compliance efforts and how to perform them; (4) WCU's record retention policy; and (5) the disciplinary consequences (including civil and criminal penalties) for non-compliance with BSA.

WCU will develop training or contract for it. Delivery of the training may include in person or virtual training, webinars, or other materials. We will maintain records to show employees are trained, the dates of training, and the subject matter of their training.

We will review our operations to see if certain employees, such as those in compliance, underwriting, policy service and benefit payment, require specialized additional training. Our written procedures will be updated to reflect any such changes.

WCU provides all agents with this AML Compliance document at the time of their initial contract signing with WCU. Agents are required to return the completed signature page of this document acknowledging their receipt and understanding of our AML policy and procedures. If the agent has a current certification from a recognized third-party training agency, the agent is asked to submit a copy of that certification to WCU.

10. Program to Independently Test AML Program

WCU will use legal counsel to interpret regulations and make recommendations for compliance.

Evaluation and Reporting

After we have completed the testing, staff will report its findings to senior management. We will address each of the resulting recommendations.

11. Confidential Reporting of AML Non-Compliance

Employees will report any potential violations of WCU's AML compliance program to the AML Compliance Officer, unless the violations implicate the AML Compliance Officer, in which case the employee shall report to the President of WCU. Such reports will be confidential, and the employee will suffer no retaliation for making them.

12. Additional Areas of Risk

WCU has reviewed all areas of its business to identify potential money laundering risks that may not be covered in the procedures described above. The major additional areas of risk include NONE.

Employee/Agent Review and Receipt

I have received and reviewed the AML Program of the Western Catholic Union and will follow the ongoing program of compliance with the requirements of the BSA and the Regulations under it.

Signature: _____ Title: _____ Date: _____

SIGN AND RETURN THIS PAGE ONLY TO WCU.
FAX: 217-223-9726 EMAIL: SALES@WCULIFE.ORG MAIL: 510 MAINE ST, QUINCY IL 62301