KGIL ANTI-MONEY LAUNDERING POLICY (AML)

POLICY STATEMENT AND PRINCIPLES

In compliance with the The Financial Intelligence and Anti-Money Laundering Act 2002 (FIAMLA 2002), the Prevention of Corruption Act 2002 (POCA 2002) and the Prevention of Terrorism Act 2002 (POTA 2002), KGILhave adopted an Anti-Money Laundering (AML) compliance policy ("Policy") as set forth in the Board minutes.

SCOPE OF POLICY

This policy applies to all KGIL officers, employees, appointed producers and products and services offered by KGIL. All business units and locations within KGIL will cooperate to create a cohesive effort in the fight against money laundering. Each business unit and location have implemented risk-based procedures reasonably expected to prevent, detect and cause the reporting of transactions required under the FIAMLA. All efforts exerted will be documented and retained in accordance with the FIAMLA. The AML Compliance Committee is responsible for initiating Suspicious Activity Reports ("SARs") or other required reporting to the appropriate law enforcement or regulatory agencies. Any contacts by law enforcement or regulatory agencies related to the Policy shall be directed to the AML Compliance Committee.

POLICY

It is the policy of KGIL 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. KGIL is committed to AML compliance in accordance with 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. For the purposes of the Policy, 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 COMMITTEE

The AML Compliance Committee, with full responsibility for the Policy shall be comprised of the General Counsel; Chief Compliance Officer, KGIL; Deputy Compliance Officer, KGIL; Assistant Vice President-Internal Audit, and Corporate Attorney. The Chief Compliance Officer shall also hold the title Chief AML Officer, and shall have authority to sign as such.The duties of the AML Compliance Committee with respect to the Policy shall include, but are not limited to, the design and implementation of as well as updating the Policy as required; dissemination of information to officers, employees and appointed producers of KGIL, training of officers, employees and appointed producers; monitoring the compliance of KGIL operating units and appointed producers, maintaining necessary and appropriate records, filing of SARs when warranted; and independent testing of the operation of the Policy. Each KGIL business unit shall appoint a contact person to interact directly with the AML Compliance Committee to assist the Committee with investigations, monitoring and as otherwise requested.

CUSTOMER IDENTIFICATION PROGRAM

KGIL has adopted a Customer Identification Program (CIP). KGIL will provide notice that they will seek identification information; collect certain minimum customer identification information from each customer, record such information and the verification methods and results; and compare customer identification information with OFAC.

KGIL®

NOTICE TO CUSTOMERS
KGIL will provide notice to customers that it is requesting information from them to verify their identities, as required by applicable law.

VERIFYING INFORMATION
Based on the risk, and to the extent reasonable and practicable, KGIL will ensure that it has a reasonable belief of the true identity of its customers. In verifying customer identity, appointed producers shall review photo identification. KGIL shall not attempt to determine whether the document that the customer has provided for identification has been validly issued. For verification purposes, KGIL shall rely on a government-issued identification to establish a customer's identity. KGIL, however, will analyze the information provided to determine if there are any logical inconsistencies in the information obtained. KGIL 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.

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 agent shall notify their New Business team. The KGIL New Business team will decline the application and notify the AML Compliance Committee.

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, KGIL will check to ensure that a person or entity does not appear on 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. KGIL shall contract with World-Check to ensure speed and accuracy in the checks. KGIL will also review existing policyholders, producers and employees against these lists on a periodic basis. The frequency of the reviews will be documented and retained. In the event of a match to the SDN List or other OFAC List, the business unit will conduct a review of the circumstances where such match has been identified. If the business unit is unable to confirm that the match is a false positive, the AML Committee shall be notified.

MONITORING AND REPORTING
Transaction based monitoring will occur within the appropriate business units of KGIL. Monitoring of specific transactions will include but is not limited to transactions aggregating $5,000 or more and those with respect to which KGIL has a reason to suspect suspicious activity. All reports will be documented and retained in accordance with the FIAMLA requirements.

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 AML Compliance Committee. Examples of red flags are:

•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 (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 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.