Gulf Insurance Group (GULF) B.S.C. (c) – Oman Branch

ANTI-MONEY LAUNDERING (AML) AND COUNTERING TERRORIST FINANCING (CTF) POLICY

Mehdi Salim Said Al Harthy, General Manager

Approved by GIG Gulf Audit, Risk, Compliance and Corporate Governance Committee in their meeting held on 06 September 2022

CONTENTS

CHAPTER 1 INTRODUCTION

Money laundering and related financial crime is a problem of global proportions and authorities estimate that more than $1 trillion in funds may be laundered globally each year. Money launderers and their colleagues often are sophisticated criminals, who quickly change their modus operandi to cope with a growing global profusion of anti-money laundering laws, regulations, and initiatives. Money laundering is not just about cash; neither is it a problem isolated to conventional deposit-taking and lending institutions and their activities. Money launderers have greatly diversified their operations across financial services sectors, including insurance sector. Primary risks include:

Compliance or regulatory risk or exposure for non-compliance with applicable existing rules and regulations;

Reputational risk stemming from money laundering "accidents" or breaches of the requirements of this Compliance manual (internal or external) and negative press coverage and associations;

Operational risk; which will manifest itself throughout operations and transactions enterprise-wide, and

Strategic risk, which can result from failure to consider money laundering vulnerability connected with mergers and acquisitions, planning and launching new products and services, entering new markets and distribution channels, and deploying new technologies.

1.1. Overview of the Requirements

The following regulations and guidelines govern the requirements relating to implementation of Anti-money Laundering (AML) & Counter Terrorist Financing (CTF) program in relation to GIG Oman's business:

- Royal Decree 30/2016 Issuing The Law of Money Laundering and Counter Terrorism Financing
- CMA Implementing Instructions of AML/CTF law (E/62/2017) for insurance companies, insurance brokers and agents
- As a branch of Bahrain incorporate company, in certain instances, the guidance will be taken from Financial Crime Rulebook issued by the Central Bank of Bahrain

In the event of any conflict between rules issued by the various regulators above, the rules issued by Royal Decree will prevail and thereafter the rules issued by Oman CMA.

1.2. AML Compliance Manual Purpose and Scope

This Anti-Money Laundering and Countering Financing of Terrorism Compliance Policy (the "Policy") is intended to provide guidance to GIG (Gulf) BSC (c) – Oman branch (hereinafter referred to as "GIG Oman " or the "Company") regarding the application of its Anti-money Laundering ("AML") policy.

The Policy was written for the GIG Gulf employees, agents and associates engaged in the operations of the company in the Sultanate of Oman.

The policy needs to be reviewed at least on an annual basis by the Branch MLRO.

1.3. Definition of Money Laundering

Money laundering is the process by which individuals or organizations attempt to conceal the true origin and ownership of the proceeds of unlawful activities. Involvement in a transaction that seeks to conceal or disguise the nature, location, source, ownership or control of proceeds derived from a wide range of

crimes may constitute money laundering. It is especially important to note that the known receipt of proceeds of unlawful activity can constitute money laundering.

While an employee or sales associate can be subject to liability when actively involved in a money laundering scheme, it is sufficient if the employee or sales associate acts to effect a transaction with the knowledge of its tainted source. Even where there is no direct evidence of such knowledge, circumstantial evidence showing that an employee or sales associate recklessly disregarded or was willfully blind to such information may be sufficient to constitute money laundering.

The following are examples of activity that could fall within the definition of money laundering or that might constitute evidence of money laundering. Additional possible indicators of suspicious activity "Red Flags" which may evidence money-laundering activity are listed in Appendix A.

- Advising a customer on how to structure a transaction to avoid reporting or recordkeeping requirements;
- Failing to report attempted large currency transactions or suspected money laundering;
- Facilitating a transaction while willfully or recklessly disregarding the source of a customer's assets or the nature of a customer's transactions;
- Concealing the source of unlawfully obtained funds by initiating and processing subsequent transfer to disguise the origin of the funds;
- Engaging in or processing a transaction with knowledge that the funds being used are derived from the proceeds of criminal activity; and
- Engaging in or processing a transaction with knowledge that the transaction is facilitating a crime.

Money laundering can involve the proceeds of a wide range of criminal activities, not only narcotics offenses. Some of these crimes include securities fraud, bank fraud, mail fraud, wire fraud, tax evasion, violation of export statutes, unlawful payments to foreign officials, illegal arms sales, robbery, racketeering, counterfeiting, kidnapping, violation of environmental laws, bribery, and terrorism. Money laundering also includes "reverse money laundering", that is using legitimate sources of funds to support terrorist or other illegal activity.

While money-laundering methods have become increasingly complex and ingenious, the "operations" continue to consist of three basic stages or processes — placement, layering, and integration:

Placement: Initial placement of funds in the financial system, without arousing suspicion;

Layering: Moving money around, often in a series of complex transactions crossing multiple jurisdictions, so that the funds are distanced from their source; and

Integration: Moving the money back into the financial and business system, so that it appears as legitimate funds or assets.

1.4. Program Compliance

Every appropriate employee and business unit must be fully aware and conversant with his or her AML responsibilities. Employees and business units are responsible to:

As soon as practicably possible, report suspicious activity, to the GIG Oman Money Laundering Reporting Officer ("MLRO"), and help ensure that the suspicious activity is properly escalated.

Know Your Customer!

Follow all policies and procedures to ensure that neither you nor GIG Gulf is put at risk by being involved or oblivious to money laundering

Carry out your record keeping or reporting responsibilities as required.

Know what is required, and personally support GIG Gulf's commitment to fully comply with the regulations.

1.5. Penalties for Non-Compliance

The company faces a huge reputational risk if it is deemed to be involved in Money Laundering related prosecution or faces regulatory censure for non-compliance with Anti-Money Laundering regulations of the Sultanate of Oman.

The element of the crime of money laundering involves "knowledge" that the funds involved in a transaction are the proceeds of illegal activity. This knowledge may not be eluded through "willful blindness" or conscious avoidance of information. One who fails to make appropriate inquiries in the face of "red flags" or other indications of possible illegal activity, and thus avoids having actual knowledge, may nevertheless be chargeable with money laundering because of willful blindness. A person does not have to know the particular type of illegal activity involved.
Financial institutions and their directors, officers and employees may be prosecuted by the regulators for assisting or participating in money laundering activities of their customers.

Persons found guilty of assisting or participating in money laundering activities are subject to regulatory penalties provided in the AML Law in Oman which include regulatory fines, imprisonment or both.

In addition, the company will also initiate disciplinary action against employees who are not in compliance with this policy. The report will be made to the audit committee which will decide on disciplinary action to be taken which could include termination from the company.

CHAPTER 2 POLICIES

As required by the AML law, GIG Gulf will follow the procedures and control measures preventing money laundering and terrorism financing which should include:

- Customer due diligence(Know Your Customer)
- Record keeping and ability to reconstruct a transaction i.e. full audit trail for the transaction
- Recognition and reporting of suspicious customers /transactions to the competent authorities
- Establishing and implementing internal policies, procedures and controls and appointment of competent officer at management level for implementation of such policies
- Establishing screening procedures when hiring employees and arranging ongoing training of employees and officers.

2.1 Money Laundering Reporting Officer

Although AML efforts are the responsibility of all employees and sales associates, the Company has designated Money Laundering Officer, (MLRO) for the Oman operations of GIG Gulf. The MLRO has to determine areas of potential money laundering risks, monitoring the Company's AML compliance, overseeing the establishment, implementation and enforcement of the Company's AML policies and procedures, education and training of employees and sales associates and communications relating to AML. The MLRO will also ensure proper AML records are kept and that required reports (such as SARs) are filed, and will be responsible for briefing senior management as appropriate. The MLRO will supervise the

Company's responses to AML-related information requests from governmental or other authorities. The MLRO may delegate certain approval or surveillance responsibilities as deemed appropriate.

Oman MLRO	**Mohammed Al Lawati**, Mohamed.Allawati@gig-gulf.com GIG Tel: (+968) 99218556
Regional MLRO	**Ajay Kumar C Compliance@gig-gulf.com**

2.2. Customer Due Diligence

Insurance licensees shall undertake customer due diligence measures (CDD) before or during the course of conducting transaction. Some of the trigger events to carry out CDD are as follows:

(a) Establishing business relation i.e. when a person applies to do business with or through them.
(b) A significant or unusual transaction takes place or an occasional transaction above specified thresholds (R.O. 6,000 for general insurance products and R.O.38,000 for life and savings products) takes place in a single operation or in several operations that appear to be linked
(c) A change in policyholders' beneficiaries is made (for instance, to include non-family members, or a request for payment to be made to person other than the beneficiaries).
(d) There is a material change in the terms of insurance policy or the manner in which the business relationship is conducted which may include any of the following:
   - Full surrender
   - Partial surrender
   - Withdrawal/prepayment of benefits in any other form
   - Lump sum top up of existing life insurance contracts
   - Increment (if the increment is for greater than 50% of the current premium)
   - Change of the type of benefit (for instance, change from an annuity to lump sum payment)
   - Change of duration (where this causes penalties)
(e) Request to use of policy as collateral security (Unless required for financing mortgagee by a reputable financial institution) i.e a temporary assignment to an authorized bank
(f) Claims, commissions and other monies are to be paid to persons other than the policyholder.
(g) In the event of an existing customer taking a new policy wherein the data provided is not in line or conflicting with the existing data held about the customer.
(h) In the event of Death claims, CDD to be done for Beneficiaries prior to payout.
(i) There is suspicion of money laundering or terrorism financing
(j) GIG Gulf has doubts about the veracity or adequacy of previously obtained customer data.

The list is not exhaustive and there could be other circumstances where there is a significant change in original terms and conditions or operating mode which may warrant a review of the CDD.

CDD should be carried out on the following persons before processing any of the requests listed below related to them:

- Policy Owner - on a trigger event only.
- Third party assignment for both Assignor & Assignee – limited to financial institutions in Oman licensed by the Central Bank of Oman (http://www.cbo-oman.org/related.htm). Care needs to be taken to check the financial institutions against World-check to ensure that they are not under sanctions (for eg, Bank Melli Iran and Bank Saderat Iran).
- Third Party Payor- can be an individual only
- Beneficiaries – only at payment stage

2.3. Customer Due Diligence (CDD) procedures

The following CDD procedures should be taken:

a) Obtaining sufficient and satisfactory evidence to establish the customers' identity and his legal existence.
b) Determining whether the customer is acting on behalf of another person, and then taking reasonable steps to obtain sufficient identification data to verify the identity of that other person and whether the customer is authorized to do so.
c) Identifying the (ultimate) beneficial owner (especially for life and other investment related insurances) and taking measures to verify the identity of the beneficial owner.
d) Obtaining information on the purpose and intended nature of business relationship
e) Conducting on going due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship.
f) Where appropriate, direct contact with the customer by phone, letter or email to confirm relevant information, such as residential address information.
g) The company may start processing the business while taking steps to verify the customers' identity. Pending receipt of required evidence, the company shall "freeze" the rights attaching to the policy, and shall not issue documents of title. In case of failure by a customer to provide satisfactory evidence of identity, the transaction in question should not proceed further and relationship be terminated. The situation must be reported to the MLRO to consider making a suspicious transaction report (STR) to the regulators.
h) In case of life insurance, where a business relationship has been established after due verification of the policyholder, it is permissible to do the identification and verification of the beneficiary after the establishment of business relationship with the policyholder. However, such identification and verification must occur before the time of payout to the beneficiary or before the time the beneficiary intends to exercise vested rights under the policy.

2.4. Methods of identification and verification for individuals:

If, customer is an individual, the company must obtain and record the following information:

a) Full name as per the clients official CDD document (eg, national ID, passport)
b) Current permanent address including postal code, and current mailing address
c) Date and place of birth (this may be city or country)
d) Nationality
e) Gender: Male/Female
f) Current Passport number and/or current National Identity Card /Resident Card number and Driving license details (for motor policies only)
g) Occupation and position held/job title
h) Employers name and address (If, self employed, the nature of self employment)
i) Telephone number, fax number, e-mail address (where applicable)
j) Signatures of the individual

The above information (a – f and j only) should be validated by collecting the following supporting documents to be obtained of the customer. Supporting docs must be in date and are valid for 6 months for those without an expiry date.

Proof of Identity (original or certified copies)	**Information Required**
• Government issued identity card (in date / must not be expired) mandatory for all applicants	• ID Number • Client Name • Date of Birth

• Passport (mandatory only for expatriates and should include copy of Oman residence permit) in date / must not be expired	• Nationality & Signature • Photograph • Place of issue • Issuing Authority • Date of issue & Expiry
Proof of residential address *(any of the following in original or a suitably certified copy)* • Utility bill or Letter from applicant's current employer on company headed paper (must be dated within 6 months of policy application / signing) • Bank Statement / Bank Credit Card Statement (must be dated within 6 months of policy application / signing) • Government issued identity card which shows the residential address in full must be in date / not expired • Proof of ownership/rental agreement of the residential address (must be dated within 6 months of policy application / signing) • Letter from applicant's bank (resident & regulated in recognized jurisdiction as per the list previously) which confirms applicant's current residential address, must be dated within 1 month of policy application / signing • Record of home visit by an official of the Company – signed and stamped on company letterhead must be dated within 1 month of policy application / signing • Some form of official correspondence from a public/governmental authority which shows full name of the applicant and full residential address – specific listing to be provided as to what is acceptable and within what date range	**Information Required** • Client Name • Complete residential address match • Issue & Expiry date • Issuing Authority / service provider • Signature

Where a person applies for a policy to insure a life other than himself/herself, it is the applicant for the policy whose identity has to be verified rather than the life to be insured.

2.5. Methods of identification and verification for legal entities (companies and other legal arrangements)

If customer is a legal entity, the insurance licensee should obtain and record the following information:

a) the entity's full name
b) date and place of incorporation and registration number
c) legal form
d) registered address and trading address
e) names, nationalities and addresses of persons owning more than 10% of the capital
f) type of business activity
g) date and place of incorporation or establishment
h) telephone, fax, e-mail address

Any documents which are not obtained and certified by an authorized official of the company should be certified and signed by any of the following from the country of residence of the applicant or GCC or FATF member state:

a) a registered notary
b) an official of any government ministry
c) an official of an embassy or consulate of the country of citizenship of the applicant
d) a chartered/certified accountant;
e) a registered lawyer
f) a manager level official of the bank (in case of bancassurance arrangements)

The individual making the certification as above must give clear contact details (e.g. by attaching a business card or company stamp). The identity of the person providing the certification must be verified through checking membership of a professional organization (for lawyers or accountants), or through checking against databases/websites, or by direct phone or email contact.

2.8. Screening and Enhanced customer due diligence for Politically-Exposed Persons (PEP)

PEPs include heads of States, senior members of the government, the judiciary, the military, or state-owned companies. PEPs also include Members of Parliaments and senior members of political parties.

GIG Gulf relies on World-check listing and data from customers to identify PEPs.
Maintaining a business relationship with a PEP or PEP family member implies enhanced due diligence measures that should be summarized in a report signed by the Country Manager, copied to the MLRO and filed in the customer file:

- **establishing the source of wealth / source of funds, to the same limits as noted in above sections**
- **stating the expected customer activity (what policies, for what amounts),**
- **detailing the existence of any foundation, trust, company or any complex financial structure used in dealing with GIG Gulf.**

Note that this report can be researched without necessarily questioning the client (PEP are not always accessible!).

The GIG senior management (country managers) should record his approval for taking on a client who is a PEP after due consideration of the potential risk for GIG Gulf.

GIG Oman MLRO will maintain a list of PEPs for continuous monitoring.

2.9. Enhanced customer due diligence for High risk and Non Cooperative Countries

This will apply to countries that the FATF has identified as jurisdictions that have strategic AML deficiencies . For list of countries, please refer Appendix D:

In relation to transactions involving any of the above countries, the same needs to be referred to the MLRO for clearance

2.10. Tracking corporate or individuals linked to terrorist organizations

i) identification of the person/s purporting to act on behalf of the customer and verification that he person/s are so authorized
j) Regulatory body or listing body (for regulated activities such as financial services and listed companies)
k) Name of external auditor (where applicable)

The information furnished shall be verified by obtaining certified copies of the following documents:
a) Certificate of incorporation/commercial registration
b) Memorandum of association
c) Articles of association
d) Partnership agreement
e) Copy of the latest financial report and accounts, audited where possible (audited copies do not need to be certified)
f) Board resolution providing the list of authorized signatories/ copies of power of attorney
g) Identification documentation of the authorized signatories.

2.6 Source of Funds & Original of Wealth

Application forms contain language which requires selling agents to certify they determined/recorded the source of the customer's assets and income (how the customer acquired or accumulated their funds). In addition, MLRO may use suitable information for enhanced due diligence on the source of funds.

Where the annual premium is in excess of threshold defined (R.O.6,000 for General insurance product and R.O. 38,000 or USD 100,000 for savings products), the origin of wealth should be verified. Some of the acceptable forms of documentation is provided in Appendix C.

Source of Funds will be required for all premiums, to confirm that the premium payments have come from the account nominated on the application form. This confirms that a third party is not paying the policy premiums.

For Life & Savings products, the following information will be collected.

Account held in Name
Bank Account Number
Swift/BIC Code
IBAN
Bank Name
Bank Postal Address
Bank Country

2.7. Certification

Any document used for the purpose of identification/verification should be original document or a copy of an original document made by an authorized official of the company (such as employee, agent or financial advisor), the copy should be dated, signed (or digitally marked) and marked 'original sighted' by the authorized official of the company.

GIG Gulf should screen its clients database for persons subject to sanctions especially those connected to terrorist organisations, as identified by the United Nations, Oman, GCC, EU, US, Canada and other applicable lists
Branch MLRO's have access to World-check login which can be used to review new clients against the sanctioned lists.

Oman branch MLRO also has access to Refinitiv system which is used for screening of customers & counterparties on a weekly and ongoing basis. Branch MLRO must investigate the alerts generated and notify Regional MLRO in case of any positive matches.

2.11. Keeping data up-to-date

The key account manager shall ensure that documents, data or information collected under the CDD process is kept up-to-date and relevant by undertaking reviews of the existing records.

2.12. Suspicious Transactions Reporting

It is a requirement and a duty for all staff members and associates who deal with the policy to report suspicious transactions. All suspicious transaction cases as well as any attempted suspicious transaction should be reported directly to GIG Oman MLRO. Remember that the obligation to report suspicious transaction is applicable not only for completed transactions but also attempted transactions.

Suspicious transaction may fall into one or more of following examples of categories:

- Any unusual financial activity or transaction of the customer
- Any unusually linked transaction
- Any unusual or disadvantageous redemption of an insurance policy
- A claim made in suspicious circumstances.
- Any unusual method of payment
- Any involvement of any person subject to international sanctions.
- An important condition for recognition of a suspicious transaction is for the insurance licensee to know enough about the customer and business relationship to recognize that a transaction or a series of transaction is unusual.
- When an insurance licensee is unable to complete CDD measures as required under this manual, MLRO should be consider making suspicious transaction report. The process of verification of customers' identity, once begun, should be pursued either to a conclusion or to the point of refusal. If a prospective policyholder does not pursue an application, this may be considered suspicious in itself.

A list of possible indicators of suspicious activities or red flags is provided in Appendix A.

2.13 Cash Payments from customers

- Not to receive any payment in cash for life insurance policies
- Not to receive any cash from legal clients for general insurance policies,except by electronic payment method
- As an exception, companies may receive the amounts in cash from individuals or companies, not exceeding 1,000 one thousand Omani riyals, for one general insurance policy
- Any cash payments from customers exceeding OMR1,000/ must be referred to branch MLRO for verification. Payment can be accepted only after the clearance from MLRO

2.14. Record Keeping

Oman Law on Money Laundering requires the institutions to maintain and hold documents of identification and addresses of customers and record of transactions for a period not less than ten years commencing the day following the finalization of transaction or closure of the account or termination of business relation, whichever is later.

GIG Gulf, therefore, is required to keep record on the risk profile of each customer and/or beneficial owner and the data obtained through the CDD process (i.e. copies of records of official identification documents like passport, identity cards, driving licenses or similar other documents), and the account files, business correspondence and record on business transactions for at least ten years after the end of business relationship i.e. at least ten years after the expiry of the policies and/or ten years after settlement of claims, surrender or cancellation. Such record should be sufficient to permit reconstruction of individual transactions so as to provide, if required, evidence for prosecution of criminal activity.

In situations, where the records relate to on-going investigations or transactions which have been subject to suspicious transaction reports, they should be retained until it is confirmed that the case has been closed.

CHAPTER 3 – TRAINING AND AWARENESS

The Company expects its employees and sales associates to maintain the integrity and professionalism of the Company and to be diligent in protecting the Company against money laundering and other illegal activity. An on-going employee-training program is a core requirement under AML regulation. It is GIG Gulf's responsibility to ensure that all appropriate employees, sales associates, and independent agents a) receive training on money laundering prevention on a regular basis (at least annually), b) fully understand relevant AML procedures and their importance, and c) fully understand that they will be committing a criminal offense if they breach provisions of the AML legislation. It is the Company's policy that periodic basic AML training and awareness will be provided, or made available, to all appropriate employees, sales associates, and independent agents. Where appropriate,, AML training will be tailored for those employees, sales associates, and independent agents who; due to the nature of their position, duties and/or exposure to risk; require enhanced training that goes beyond the AML training generally provided. The status of the AML training and awareness programs is reported to Senior Management at least annually.

3.1. New Hire Orientation

The Company's orientation program for all new employees includes an overview of the Company's AML Program which is provided by the MLRO. All new employees also registered for an e-learning program which is mandatory and to be completed before end of the probation period or 3 months whichever is earlier. The new employees will also receive access to the Company's AML/CTF Policy on the intranet. At least on an annual basis, the staff must undergo refresher training on AML.

3.2. Sales Associates, financial advisors, independent agents and other applicable persons

The Company will also provide access to the AML and Compliance e-learning to Sales Associates, financial advisors, independent agents and other applicable persons (for eg, providing outsourced services for the Company, contract/temporary staff). These persons will also have to undergo refresher training on AML on an annual basis.

3.3. Training Components

The components of AML training will be managed by the MLRO in coordination with the Learning and Development team. The content will be changed as AML regulatory guidance is modified and enhanced.

Changes are also made to the training program curriculum and medium to keep it informative and interesting. The components will continually contain AML scenarios sample of red flags, record keeping and escalation requirements and penalties for non-compliance.

3.4. Senior Management Awareness

The MLRO meets with the Senior Management and ensure they are aware of the AML requirements and their responsibilities in implementing the program effectively and to set the tone at the top.

3.5. MLRO Training

The MLRO must in coordination with the regional office ensure that they are kept updated on the developments on AML and where necessary attend AML Conference hosted by a reputable organization, unless budget constraints do not permit it. It also enables the staff to obtain information from various vendors and ask questions about current industry standards regarding various aspects of the Regulations.

APPENDIX – A – Possible indicators of suspicious activity ("RED FLAGS")

All employees and business units should be aware of "Red Flags" of money laundering. While no one criterion may be a definitive indicator of money laundering activity, the following are examples of suspicious activity that should prompt additional scrutiny for money laundering risks. This list should not to be considered all-inclusive. The list has been separated into two categories - New Business and In-Force Activity. However, all categories should be referenced because some of the indicators are applicable to more than one area.

New Business

- A customer attempts to purchase a policy or annuity or to make an investment in an amount that is beyond the customer's apparent means, that has no purpose, or where the source or nature of funds to be used is suspicious
- A customer shows greater interest in the early surrender or cancellation provisions of a product rather than its investment performance/return
- A customer exhibits concern regarding the firm's AML procedures and/or compliance with 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
- A customer has difficulty describing the nature of his or her business or lacks general knowledge of his or her industry.
- A customer previously unknown to the sales associate who asks for expeditious handling and indicates an intention to invest a significant amount of money
- 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 of funds and other assets
- The customer exhibits a lack of concern regarding risks, commissions, or other transaction costs
- The customer is from, or has accounts in, a country identified as a non-cooperative country or territory by the Financial Action Task Force (FATF)
- Situations where verification of identity is difficult
- Introduction of a customer by an overseas associate or financial institution based in a country or jurisdiction known for drug trafficking and production and other financial crime as provided in Appendix D

APPENDIX A. Possible indicators of suspicious activity - continued

- Insurance policies with values that appear to be inconsistent with the buyer's insurance needs
- Forming companies or trusts with no apparent business purpose
- Customer furnishes unusual or suspect business documents or identification
- Customer, or associated person, has a questionable background or is the subject of news reports indicating possible crime, civil or regulatory violations
- The designated beneficiary has no relationship to the policyholder
- Customer is acting as an agent for a principal and is reluctant to provide information about that person/entity
- New account forms taken on a non face-to-face basis (i.e., form taken by mail or over the phone) when it would not be customary to receive forms in this manner
- Addresses unrelated to the clients
- Policy coverage inconsistent with ability to pay premium
- Multiple accounts under the same name or multiple names
- Insistence on use of P.O. Box address or mailing address instead of a street address
- Presentation of money orders from numerous payor sources for initial investment
- Assignment of benefits to unrelated party to the policyholder
- Customer cashes out of annuities during the "free look" period or surrenders early
- Agents and agencies that continually submit cases that result in free look cancellation, surrender within the first year, etc..
- Individual is associated with a person linked to document forgery
- Individual refuses to provide required information or misrepresents details in order to make information difficult to verify
- Apparent unusual concern for secrecy regarding personal identity, occupation, type of business or property held
- Displays high level or curiosity about internal systems, policies and controls
- Appears nervous, secretive, reluctant to meet in person; over justifies or explains a transaction

APPENDIX A Possible indicators of suspicious activity – continued

In-Force Activity

- A customer seeks to cancel a life insurance policy prior to maturity without regard to penalties or cancels more than one policy during the free look period
- Premium payments made with multiple cash equivalents (bank check, cashier check, money order) purchased from the same and/or different financial institutions
- Any accounts identified, either during the account opening process or through subsequent review, where there is no apparent relationship between the owner and the insured or annuitant
- A customer attempts to make frequent or large deposits of currency, insists on dealing only in cash equivalents or asks for exemptions to the firm's policies relating to the deposit of cash and cash equivalents
- A customer's account has unexplained or sudden extensive wire activity, where previously there had been little or no wire activity without any apparent business purpose
- A customer makes a 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
- A customer makes a deposit, for the purpose of purchasing a long-term investment, followed shortly thereafter by a request to liquidate the position and a transfer of the proceeds out of the account
- For no apparent reason, a customer has multiple accounts under a single name or multiple names, with a large number of inter-account or third-party transfers
- A customer requests that a transaction be processed in such a manner so as to avoid the firm's normal documentation requirements
- Transactions that appear inconsistent with a customer's known legitimate (business or personal) activities or means; unusual deviations from normal account and transaction patterns
- Large or unusual currency settlements for investments or payment for investments made from an account that is not the customer's
- Transactions passed through intermediaries for no apparent business reason
- Uncharacteristically premature redemption of investment vehicles, particularly with requests to remit proceeds to apparently unrelated third parties
- The purchase of large cash value investments, soon followed by heavy borrowing against them
- Large lump-sum payments from abroad
- Insurance policies with premiums or top-ups that exceed the buyer's apparent means
- Payor of the premium is not the policyholder and does not seem to be related to the policyholder.

APPENDIX A. Possible indicators of suspicious activity – continued

- Address "in care of (c/o)" of a third party
- High level of loan activity within a short period of time (i.e., three loans taken in a calendar year)
- A request for payment is made by an individual who is not the owner, insured or beneficiary
- Early termination of a policy, especially at a loss, where cash was tendered and/or the refund cheque is directed to the third party and policyholder is unconcerned about the early surrender charge
- Customer changes addresses frequently
- Engages in sudden withdrawal of funds or closes account(s) with subsequent wire transfers to foreign accounts
- Multiple suspicious financial activity originating from or terminating at the same location
- Known terrorism-associated charity or relief organization linked to transaction(s)
- Changes in patterns of transactions, including trading on financial and commodities markets

APPENDIX B - Form for reporting Internal Suspicious Transactions

GIG INURANCE (GULF) BSC (c)

Branch: _____

In Respect of: ☐ Individual ☐ Company / Business

Date of transaction/attempted transaction:

1. Full Name of Client	
2. Nationality	
3. CR No. / ID No. / Passport No.	
4. Full Permanent address	
5. Date of Birth / Date of Incorporation	
6. Occupation / Business activity	
7. Contact Person & Designation (for companies)	
8. Telephone number;	
9. Fax number;	
10. E-mail address	
11. Website (if available)	
12. Profession	
12. Source of Income	

Documents Collected	

Transaction Details

Policy details:
Reason for Suspicion/Reporting (attach additional sheets if required and note number of pages attached)

Name and Signature of Employee reporting **Date**

Comments by Branch MLRO and signature	Date

APPENDIX C - Verification of Source of income/wealth where the total premium payments exceed above specified thresholds
(R.O. 6,000 for general insurance products and R.O.38,000 for life and savings products)

Agreed Origin of Wealth information	**Documentary Evidence** *(documents submitted should either be original or a copy certified by a suitable certifier)*
Income p.a. and/or bonus amount	• Certified copy of recent financial accounts or Income tax assessment document if self-employed **or** • Confirmation from employer of income on letter headed paper which must be an original **or** • Bank statements clearly showing receipt of most recent regular salary payments covering three months from named employer
Shares or other investments holdings	• Investment holdings/savings certificates, contract notes or statements **or** • Confirmation from the relevant investment company **or** • Signed letter detailing funds from a regulated accountant • Bank statement showing receipt of funds by investment company
Property sale	• Signed letter from lawyer **or** • Signed letter from estate agent (if applicable) **or** • Sale contract
Maturing investments or policy claim	• Letter from previous investment company re notification of proceeds of claim
Company sale	• Signed letter from lawyer **or** • Signed letter from regulated accountant **or** • Copy of contract of sale and sight of investment monies on bank statement
Inheritance	• Grant of probate (with a copy of the will) which must include the value of the estate **or** • Lawyer's letter or letter from trustees of an estate • Shariah court order
Gift	• Letter from donor confirming details of gift **and** Certified copy of the donor's primary ID documentation **and** Suitable documentation to evidence the donor's origin of wealth (as per the origin of wealth guidelines)
Compensation payment	• Letter/Court order from compensating body **or** • Lawyer's letter
Corporate investments	• Reports and accounts **or** • Accountant confirmation of nature of business and turnover
Retirement income	• Pension statement **or** • Letter from accountant **or** • Bank statements **or** • Savings account statement
Other monies	• Appropriate supporting documentation **or** • Signed letter detailing funds from a regulated accountant

APPENDIX D – High Risk Jurisdictions and Jurisdictions under Increased Monitoring
As of June 2022 there are no countries on the NCCT list

https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/increased-monitoring-june-2022.html

High Risk Jurisdictions
High-risk jurisdictions have significant strategic deficiencies in their regimes to counter money laundering, terrorist financing, and financing of proliferation. For all countries identified as high-risk, the FATF calls on all members and urges all jurisdictions to apply enhanced due diligence, and in the most serious cases, countries are called upon to apply counter-measures to protect the international financial system from the ongoing money laundering, terrorist financing, and proliferation financing (ML/TF/PF) risks emanating from the country. This list is often externally referred to as the "black list" Iran Democratic People's Republic of Korea (DPRK) Jurisdictions under increased monitoring are actively working with the FATF to address strategic deficiencies in their regimes to counter money laundering, terrorist financing, and proliferation financing. When the FATF places a jurisdiction under increased monitoring, it means the country has committed to resolve swiftly the identified strategic deficiencies within agreed timeframes and is subject to increased monitoring. This list is often externally referred to as the "grey list". Albania Barbados Burkina Faso Cambodia Cayman Islands Haiti Jamaica Jordan Mali Malta Morocco Myanmar Nicaragua Pakistan Panama Philippines Senegal South Sudan Syria Turkey Uganda United Arab Emirates Yemen