NATIONAL COUNCIL FOR
LAW REPORTING
LIBRARY

LEGAL NOTICE NO. 23

THE INSURANCE ACT

(Cap. 487)

THE INSURANCE (ANTI-MONEY LAUNDERING AND COMBATING FINANCING OF TERRORISM) GUIDELINES, 2020

IN EXERCISE of the powers conferred by section 3A (g) of the Insurance Act, the Insurance Regulatory Authority issues the following guidelines—

Citation.

1. These guidelines may be cited as the Insurance (Anti-Money Laundering and Combating Financing of Terrorism) Guidelines, 2020.

Interpretation.

2. In these guidelines, unless the context otherwise requires—

"Act" means the Insurance Act;

"Authority" refers to Insurance Regulatory Authority;

"beneficiary" refers to the beneficiary to the insurance contract;

No. 9 of 2009.

"Centre" refers to the Financial Reporting Centre established under section 21 of Proceeds of Crime and Anti-Money Laundering Act, 2009;

"customer" refers to a policyholder or prospective policyholder;

"money laundering" has the same meaning as provided for under the Proceeds of Crime and Anti-Money Laundering Act, 2009;

L.N. 59/2013.

"politically exposed persons" has the same meaning as defined in the Proceeds of Crime and Anti Money Laundering Regulations, 2013; and

"regulated entity" refers to insurers, takaful operators and microinsurers underwriting life assurance; brokers and agents licensed under the Act.

Object of the guidelines.

3. (1) The object of these guidelines shall be to outline the requirements for regulated entities to develop programmes to effectively combat money laundering and financing of terrorism activities.

Application of the guidelines.

4. These guidelines shall apply to regulated entities.

General requirements for regulated entities.

5. (1) A regulated entity shall establish and maintain a anti-money laundering and combating financing of terrorism program including comprehensive risk assessment, screening process and controls to mitigate any risks arising from money laundering or financing of terrorism.

(2) A regulated entity shall adopt policies on anti-money laundering and combating financing of terrorism for the prevention of transactions that may facilitate money laundering or financing of terrorism.

(3) A regulated entity shall formulate and implement internal procedures and other controls to deter criminals from using its services and products for money laundering and financing of terrorism.

Responsibilities of the board of a regulated entity.

6. The board of a regulated entity shall—

(a) establish policies and procedures for the prevention, detection, reporting and control of money laundering and financing of terrorism activities; and

(b) promote a strong risk and compliance culture and develop monitoring and reporting mechanisms to support anti-money laundering and combating financing of terrorism controls.

Responsibilities of the management of a regulated entity.

7. The management of a regulated entity shall—

(a) develop, implement and issue to its staff instruction manuals setting out procedures for—

(i) customer acceptance and identification;

(ii) customer due diligence;

(iii) record-keeping;

(iv) identification and reporting of suspicious transactions;

(v) staff screening and training; and

(vi) establishing legitimate sources of funds;

(b) ensure that the internal audit or compliance function regularly verifies compliance with anti-money laundering and financing of terrorism policies, procedures and controls;

(c) assess and ensure that the risk mitigation procedures and controls work effectively;

(d) register with the Centre and comply with the any reporting requirements;

(e) report to the Centre suspicious transactions; and

(f) appoint a Money Laundering Reporting Officer.

Money laundering reporting officers.

8. (1) A regulated entity shall appoint a person in management as a Money Laundering Reporting Officer who shall have relevant competence, authority and independence.

(2) Other than in the case of a sole proprietor, a principal officer and internal auditor of a regulated entity shall not qualify to be appointed as a Money Laundering Reporting Officer.

Functions of the money laundering officer.

9. A Money Laundering Reporting Officer of a regulated entity shall—

(a) co-ordinate the development of a programme on anti-money laundering and combating financing of terrorism compliance;

(b) monitor, review and co-ordinate the implementation of the anti-money laundering and combating financing of terrorism compliance program;

(c) receive and vet suspicious transaction reports from the regulated entity's staff;

(d) submit suspicious transaction reports to the Centre;

(e) co-ordinate the training of staff in anti-money laundering and combating financing of terrorism awareness, detection methods and reporting requirements;

(f) together with the human resources function, ensure that new members of staff are screened; and

(g) act as a liaison officer for the Authority and Centre and a point of contact for all employees on issues relating to money laundering and financing of terrorism.

Access to information.

10. A regulated entity shall ensure that the Money Laundering Reporting Officer has access to other information that may be of assistance to the officer in respect of suspicious or unusual transaction reports.

Independent audits.

11. (1) The board of a regulated entity shall ensure that—

(a) annual independent audits of the internal anti-money laundering and combating financing of terrorism measures are undertaken to determine their effectiveness;

(b) that the roles and responsibilities of the auditor are clearly defined and documented including—

(i) checking and testing compliance with relevant legislations on money laundering and financing of terrorism; and

(ii) assessing whether current measures are consistent with developments and changes of anti-money laundering and combating financing of terrorism requirements.

(2) The auditor shall submit a written report on the audit findings to the board highlighting any inadequacies in internal anti-money laundering and combating financing of terrorism measures and controls and the board shall ensure that necessary measures are taken to rectify the inadequacies.

(3) A board of a regulated entity shall ensure that audit findings and reports are submitted to the Authority within thirty days of receiving the findings or reports but in any event not later than the 31st January of every year.

Anti-money laundering and combating financing of terrorism programme.

12. (1) A regulated entity shall establish and maintain an anti-money laundering and combating financing of terrorism program that sets out the internal policies, procedures and controls necessary to detect money laundering and financing of terrorism and to manage and mitigate the risk of money laundering and financing of terrorism.

(2) An anti-money laundering and combating financing of terrorism program shall include—

(a) the appointment of a Money Laundering Reporting Officer;

(b) the development and regular review of internal policies, procedures and controls;

(c) assessment and documentation of risks related to money laundering and financing of terrorism, and the documentation and implementation of mitigation measures to deal with the risks;

(d) continuing training for employees and agents; and

(e) an independent review of the policies, procedures and internal controls to test their effectiveness and efficiency.

(3) A money laundering and financing of terrorism program shall take into account the nature, scale and complexity of the regulated entity and the nature and degree of money laundering and financing of terrorism risks facing the entity.

(4) The money laundering and financing of terrorism program shall be documented, approved by the board and communicated to all levels of the regulated entity.

Elements of anti-money laundering and combating financing of terrorism

13. A regulated entity shall develop and maintain an anti-money laundering and combating financing of terrorism policy which including—

(a) a high-level summary of key controls and objectives of the policy;

(b) a statement that the anti-money laundering and combating financing of terrorism policy applies to all areas of the business including on a global basis—

(i) to waivers and exceptions; and

(ii) to operational controls.

Key operational controls of an anti-money laundering and combating financing of terrorism policy.

14. The operational controls of an anti-money laundering and combating financing of terrorism policy shall include—

(a) a statement of responsibility for compliance with the anti-money laundering and combating financing of terrorism policy;

(b) customer due diligence including—

(i) customer identification and verification;

(ii) additional Know Your Customer information;

(iii) high-risk customers;

(iv) non-face-to-face business, where applicable;

(v) reinsurance arrangements;

(vi) the handling of politically exposed persons;

(vii) monitoring and reporting of suspicious transactions;

(vii) co-operation with other relevant authorities;

(ix) record-keeping;

(x) screening of transactions and customers;

(xi) employee training and awareness; and

(xii) adoption of risk management practices and use of a risk-based approach.

Compliance policy statement.

15. A regulated entity shall develop a compliance policy statement on the commitment of senior management and board of the entity to develop anti-money laundering and combating financing of terrorism objectives and implementation of measures to deter the use of its services and products for money laundering and financing of terrorism.

Content of compliance policy statement.

16. (1) An anti-money laundering and financing of terrorism policy shall establish clear responsibilities and accountabilities within the regulated entity to ensure that policies, procedures and controls are developed and maintained to deter criminals from using their services and products for money laundering and financing of terrorism.

(2) An anti-money laundering and financing of terrorism policy shall include—

(a) standards and procedures for compliance with applicable laws and regulations;

(b) a description of the role of the Money Laundering Reporting Officer and other relevant employees;

(c) screening programs for hiring employees;

(d) incorporating anti-money laundering compliance in job descriptions and performance evaluations of appropriate employees;

(e) mechanisms for program continuity when there are changes in management or employee composition or structure; and

(f) any other issue as may be required by the Authority

Compliance policy.

17. The compliance policy statement shall include a statement that—

(a) employees shall comply with applicable laws and regulations and corporate ethical standards;

(b) activities by the regulated entity shall comply with applicable laws and regulations;

(c) directs staff to a compliance officer or other knowledgeable individual when there is a question regarding compliance matters; and

(d) employees shall be held accountable for carrying out their compliance responsibilities.

Staff vetting.

18. A regulated entity shall establish—

(a) screening procedures when hiring employees and agents taking into account the risks identified in the entity's risk assessment; and

(b) policies, procedures and controls for the regular vetting senior managers, the Money Laundering Reporting Officer and any other employee whose role involves anti-money laundering and combating financing of terrorism duties.

Training.

19. (1) A regulated entity shall establish measures to ensure that the members of the board, employees and agents are regularly trained on—

(a) anti-money laundering and combating financing of terrorism laws and regulations;

(b) prevailing techniques, methods and trends in money laundering and financing of terrorism; and

(c) the entity's internal policies, procedures and controls on anti-money laundering and financing of terrorism.

(2) A regulated entity shall document and maintain the following in respect of training—

(a) scope and nature of the training;

(b) the tasks to be undertaken by staff who have had anti-money laundering and financing of terrorism training;

(c) application of the anti-money laundering and financing of terrorism training, including frequency and delivery methods;

(d) monitoring to ensure that members of staff have completed the required training;

(e) tailoring training for different employees based on tasks carried out and degree of anti-money laundering and financing of terrorism risk the entity faces from members of staff in their positions; and

(f) whether and how employees are assessed for knowledge, application and retention of the anti-money laundering and financing of terrorism training.

Risk assessment.

20. A regulated entity shall—

(a) conduct a risk assessment of its customers to identify the type of customers with a high risk of money laundering and financing of terrorism;

(b) establish measures in its internal policies and procedures to address the different kinds of risks posed by its customers;

(c) apply a risk-based approach in the assessment of risks associated with money laundering and financing of terrorism in respect to—

(i) customers and business relationships;

(ii) products and services;

(iii) distribution channels;

(iv) geographical location; and

(v) other relevant factors;

(d) take into consideration the following factors when conducting risk assessment of customers or type of customers—

(i) the origin of the customer and location of business;

(ii) background of the customer;

(iii) nature of the customer's business;

(iv) structure of ownership for a corporate customer; and

(v) any other information that may indicate whether or not the customer is of higher risk;

(e) monitor the patterns of each customer's transactions to ensure it is in line with the customer's profile and reassess the customer's risk profile if there are material changes;

(f) incorporate the following in its risk assessment and profiling processes—

(i) documentation on risk assessment and findings;

(ii) consider all relevant factors before determining the level of overall risk and appropriate level and type of mitigation to be applied;

(iii) ensure that risk assessment procedures are up to date; and

(iv) conduct an assessment at least once every two years;

(g) take enhanced measures to manage and mitigate high risks;

(h) apply simplified mitigation measures for low risks;

(i) document the outcome of risk assessment and submit the report the Authority upon request.

Customer due diligence.

21. (1) A regulated entity shall—

(a) conduct customer due diligence and establish the identity and legal existence of customers based on reliable and independent source documents; and

(b) conduct customer due diligence when—

(i) establishing business relationship with a customer;

(ii) carrying out cash or occasional transactions;

(iii) the entity suspects money laundering or financing of terrorism activities; or

(iv) the entity doubts the correctness or adequacy of previously obtained information.

(2) The customer due diligence shall comprise of—

(a) identifying and verifying relevant customer details;

(b) identifying and verifying beneficial ownership and control of transactions;

(c) identifying and verifying any natural persons behind a legal person or legal arrangement including the nature of business, ownership and control structure in relation to a customer that is a legal person or legal arrangement;

(d) obtain information on the purpose and intended nature of the business relationship or transaction; and

(e) conduct on-going due diligence and scrutiny to ensure that the information provided is up to date and relevant.

(3) A regulated entity shall—

(a) take reasonable steps to ascertain the true identity of its customers or beneficiaries;

(b) identify and verify details of proposed recipients where claims and other monies are payable to persons or companies other than customers or beneficiaries; and

(c) not commence business relationships or perform any transactions or, in the case of existing business relationships, renew such business relationships where customers fail to comply with customer due diligence requirements and file suspicious transaction reports with the Centre where necessary.

(4) A regulated shall conduct customer due diligence for not more than fourteen days after the business relationship has been established where the risks of money laundering and financing of terrorism are low or where measures are already in place to effectively manage the risk to enable the customer to furnish the relevant documents.

(5) Where a regulated entity has already commenced the business relationship and is unable to ascertain the identity of the customer or beneficiary, it shall terminate the business relationship and make a suspicious transaction report to the Centre.

Simplified customer due diligence.

22. A regulated entity may apply simplified customer due procedures where there is no suspicion of money laundering or financing of terrorism and—

(a) where the risk profile of the customer is low;

(b) there is adequate public disclosure in relation to the customer; or

(c) there are adequate checks and controls from the customer's country of origin or source of funds.

Enhanced customer due diligence.

23. (1) A regulated entity shall apply enhanced customer due diligence procedures in order to—

(a) obtaining further information that may assist the entity in ascertaining the customer's identity;

(b) verify the documents furnished by the customer;

(c) obtain senior management approval for establishing business relationship;

(d) obtain comprehensive customer profile information including the purpose for the insurance cover, the occupation of the customer and source of funds;

(e) assign a member of staff to serve, and conduct continuous due diligence of, the customer;

(f) request other documents to complement those which are otherwise required; and

(g) request certification of submitted documents by appropriate authorities or professionals.

Information on natural person.

24. (1) A regulated entity shall, in the case of a natural person, require the customer to produce an official record to ascertain the true identity seeking to enter into a business relationship, such as—

(a) a birth certificate;

(b) a national identity card;

(c) a driver's licence;

(d) passport; or

(e) such other particulars as may be required by the Financial Reporting Centre under section 44 of the Proceeds of Crime and Anti Money Laundering Act, 2009. No. 9 of 2009.

(2) A regulated entity may take additional measures to identify and verify the identity of the customer including the customer's—

(a) postal address;

(b) physical or residential address;

(c) utility bills including electricity or water bills;

(d) occupation or employment details;

(e) source of income;

(f) nature and location of business activity;

(g) personal identification number issued under a tax law;

(h) where applicable, written references attesting to the customer's identity;

(i) such other particulars as may be required by the Financial Reporting Centre under section 44 of the Proceeds of Crime and Anti Money Laundering Act, 2009 or any other written law.

Information on legal persons.

25. A regulated entity shall obtain the following documents from a legal person or a body corporate when conducting customer due diligence—

(a) its registered name;

(b) a certified copy of its Certificate of Registration or Certificate of Incorporation, or Memorandum and Articles of Association or other similar documentation;

(c) a certified copy of its board's resolution granting authority to transact business with the regulated entity and designating persons having signatory authority thereof;

(d) the names, dates of birth, identity card or passport numbers and addresses of the natural persons managing, controlling or owning the body corporate or legal entity;

(e) in the case of corporate bodies, the audited financial statements for the year preceding the transaction with the regulated entity;

(f) its personal identification number issued under a tax law; or

(g) where applicable, written confirmation from the customer's prior regulated entity, attesting to the customer's identity and previous business relationship.

Information on partnerships.

26. A regulated entity shall obtain the following particulars to ascertain the identity of a partnership—

(a) the name of the partnership or its registered name;

(b) the partnership deed;

(c) the registered address or principal place of business or office;

(d) the registration number;

(e) the names, dates of birth, identity card numbers or passport numbers and addresses of the partners;

(f) the partner who exercises executive control in the partnership;

(g) the name and particulars of the natural person who has been authorised to establish a business relationship or to enter into a transaction with the regulated entity on behalf of the partnership; or

(h) the un-audited financial statements for the year preceding the transaction with the regulated entity.

Information on trusts.

27. A regulated entity shall obtain the following particulars to ascertain the identity of a trust—

(a) its registered name, if any;

(b) its registration number, if any;

(c) its Certificate of Incorporation or registration, where relevant;

(d) the trust deed;

(e) official returns indicating its registered office and, where different from the registered office, the principal place of business;

(f) the names and details of the management company of the trust or legal arrangement, if any;

(g) the names of the persons having senior management position in the legal person or trustees of the legal arrangement;

(h) names of the trustees, beneficiaries or any other natural person exercising ultimate effective control over the trust;

(i) the name of the founder of the trust;

(j) any other documentation from a reliable independent source proving the name, form and current existence of the customer; and

(k) such other documents or particulars as may be required by the Financial Reporting Centre under section 44 of the Proceeds of Crime and Anti Money Laundering Act, 2009. No. 9 of 2009.

Ascertainment of ultimate beneficiaries.

28. (1) A regulated entity shall ascertain the beneficial owners, nature of business ownership and control structure of corporate customers and sources of funds of the customer.

(2) A regulated entity shall obtain the following particulars to ascertain the beneficial owners and control structure of corporate customers—

(a) details of incorporation;

(b) partnership agreements;

(c) deeds of trust;

(d) particulars of directors and shareholders;

(e) names of relevant persons holding senior management positions;

(f) names of trustees, beneficiaries or any other natural person exercising ultimate effective control; and

(g) any other documentation obtained from a reliable independent source ascertaining the name, form and existence of the customer.

(3) A regulated entity shall conduct customer due diligence on any natural person who ultimately owns or controls the customer's transaction if it suspects that a transaction is conducted on behalf of a beneficial owner and not the person who is conducting the transaction.

Reliance on intermediaries for customer due diligence.

29. (1) A regulated entity may rely on customer due diligence conducted by intermediaries if it is satisfied that the intermediary—

(a) has adequate customer due diligence procedures;

(b) has reliable mechanisms for verifying customer identities;

(c) can provide the customer due diligence information and readily make copies of relevant documentation available on request; and

(d) is regulated and supervised for the purpose of preventing money laundering and financing of terrorism.

(2) A regulated entity that relies on an intermediary for customer due diligence shall not be required to retain copies of customer identification documentation where the documentation can be obtained from the intermediary on request.

(3) Where a regulated entity relies on an intermediary for customer due diligence, ultimate responsibility for customer due diligence shall remain with the regulated entity.

New technologies and non-face-to-face transactions.

30. (1) A regulated entity shall take reasonable measures to mitigate money laundering and financing of terrorism risks arising from the use of new technologies in transactions which do not require face-to-face contact.

(2) A regulated entity shall establish measures for customer verification that are as stringent as those for face-to-face interactions and implement monitoring and reporting mechanisms to identify potential money laundering and financing of terrorism activities.

(3) A regulated entity shall, where possible, carry out face to face interviews for high risk customers.

(4) A regulated entity shall only establish business relationships upon completion of the customer due diligence process that have been conducted through face-to-face interactions.

(5) A regulated entity shall apply customer identification procedures and continuing monitoring standards for non-face-to-face customers as for face-to-face customers

(6) A regulated entity shall take any of the following measures to mitigate the risks associated with non-face-to face transactions—

(a) require certification of identity documents by magistrates, legal practitioners, commissioners of oaths or notaries public;

(b) requisition of additional documents to complement those required for face-to-face customers;

(c) use independent contacts to verify customer identities;

(d) require payment of premiums through a bank account in the customer's name;

(e) require more frequent update of information on customers; or

(f) refusal of business relationships without face-to-face contact for high risk customers.

Politically exposed persons.

31. (1) A regulated entity shall have, in addition to its customer due diligence process, a risk management framework to ascertain whether or not customers are politically exposed persons.

(2) A regulated entity shall gather sufficient and appropriate information from the customer and any other source to ascertain whether or not the customer is a politically exposed person.

(3) A regulated entity shall take reasonable measures to establish the source of funds of a politically exposed person with whom it has a business relationship.

(4) A regulated entity shall conduct enhanced continuing customer due diligence on politically exposed persons during its business relationships with politically exposed persons including customer due diligence on the family members or close associates of politically exposed persons.

Higher risk customers.

32. (1) A regulated entity shall conduct enhanced customer due diligence on customers assessed as higher risk including requiring—

(a) more detailed information from the customer and other sources including the purpose of the transaction and source of funds; and

(b) approval from the senior management of the regulated entity before establishing the business relationship with the customer.

(2) Customers assessed as higher risk include—

(a) high net worth individuals;

(b) non-resident customers from locations known for high rates of crime and higher risk jurisdictions as identified under section 45A of the Proceeds of Crime and Anti Money Laundering Act, 2009; No. 9 of 2009.

(c) politically exposed persons;

(d) legal arrangements that are complex including trusts and nominees;

(e) cash-based businesses; and

(f) unregulated industries.

Beneficiaries of life insurance contracts.

33. A regulated entity shall, in addition to customer due diligence on customers and beneficial owners, conduct customer due diligence on beneficiaries of life insurance and other investment related insurance policies as soon as the beneficiaries are identified or designated.

Record-keeping.

34. (1) A regulated entity shall ensure that customer records including the customer profiles are up to date and relevant.

(2) A regulated entity shall regularly review customer records, especially when—

(a) a significant transaction takes place;

(b) there is a material change in the way the customer account is operated;

(c) the customer's documentation standards change substantially; or

(d) the entity discovers that the customer information is or has become inadequate.

(3) A regulated entity shall maintain customer records for at least seven years after the end of the business relationship and ensure that that the information is easy to retrieve.

(4) The customer records to be maintained include—

(a) the risk profile of customers or beneficiaries;

(b) data obtained through customer due diligence;

(c) the nature and date of transactions;

(d) the type and amount of currency involved;

(e) the policy and claims settlement details, statements of account and business correspondence; and

(f) copies of official documents of identity such as passports, identity cards or similar documents.

(5) Where customer records are the subject of ongoing investigations or prosecution in court, they shall be retained beyond the

specified retention period until it is confirmed by the relevant authority that the records are no longer needed.

(6) A regulated entity shall ensure that all documents collected through customer due diligence are up to date and relevant by conducting reviews of existing records.

Audit trails.

35. A regulated entity shall ensure that retained documents and records—

(a) are able to create a traceable audit trail on individual transactions;

(b) can enable the entity to establish the history, circumstances and reconstruction of each transaction including the—

(i) identity of the customer or beneficiary;

(ii) type and form of transaction; and

(iii) amount and type of currency;

(c) are in a form that is acceptable under the Evidence Act; and Cap. 80.

(d) are secure and retrievable in a timely manner.

Ongoing monitoring.

36. (1) A regulated entity shall conduct continuing customer due diligence with regards to its business relationship with its customers, account activities and transaction behaviour based on customer risk assessments.

(2) A regulated entity shall conduct continuing due diligence on existing high-risk customers including endorsements to policies and exercise of rights under terms of insurance contracts.

(3) Transactions which a regulated entity shall be required to conduct continuing due diligence on existing high-risk customers include—

(a) change in beneficiaries to include non-family members;

(b) request for payments to persons other than beneficiaries;

(c) a significant increase in the sum insured or premium payment that appears unusual in the light of the income of the policy holder;

(d) use of cash for payment of large single premiums;

(e) payment by a wire transfer from or to foreign parties;

(f) high frequency of endorsements on a policy;

(g) payment by banking instruments which allow anonymity of the transaction;

(h) change of address or place of residence of the policy holder or beneficiary;

(i) lump sum top-ups to an existing life insurance contract;

(j) lump sum contributions to personal pension contracts;

(k) requests for prepayment of benefits;

(l) unusual use of the policy as collateral other than for the financing of a mortgage by a regulated financial institution;

(m) change of the type of benefit including change of type of payment from an annuity to a lump sum payment; or

(n) early surrender of the policy or change of the duration where this causes penalties or loss of tax relief.

(4) A regulated entity shall conduct continuing customer due diligence to ascertain the economic background and purpose of any transaction or business relationship that appears unusual, does not have any apparent economic purpose or the legality of such transaction is not clear including with regards to complex and large transactions or higher risk customers.

(5) A regulated entity shall conduct continuing due diligence or monitoring of transactions of business relationships and transactions with individuals, businesses, companies and financial institutions from countries which have insufficiently implemented anti-money laundering and combating financing of terrorism measures.

(6) A regulated entity shall make further enquiries on such business relationships and transactions including their background and purpose and document the findings in writing.

Management information system.

37. (1) A regulated entity shall put in place an adequate management information system to complement its customer due diligence and which should provide the entity with timely information on a regular basis to enable the entity to detect any suspicious activity.

(2) The management information system shall be part of the regulated entity's information system that contains its customers' normal transaction and business profile, which is accurate and updated.

Suspicious transactions.

38. (1) A regulated entity shall establish internal criteria, hereafter referred to as red flags, to detect suspicious transactions and for conducting enhanced due diligence and continuing monitoring of any transaction that matches the red flags criteria.

(2) Suspicious transactions may fall in any of the categories specified in the Schedule.

Suspicious transactions reporting.

39. A regulated entity shall—

(a) report suspicious transactions to the Centre and maintain a register of reported suspicious transactions;

(b) ensure that the reporting of suspicious transactions is done securely in order to maintain confidentiality and secrecy.

Triggers for submission of suspicious transactions reports.

40. (1) A regulated entity shall submit a suspicious transaction report when—

(a) it is unable to complete the customer due diligence process on a customer who is unreasonably evasive or uncooperative based on normal commercial criteria and its internal policy; or

(b) a customer's transaction or attempted transaction fits the regulated entity's list of red flags.

(2) The Money Laundering Reporting Officer of a regulated entity shall maintain a register of internally generated suspicious transaction reports and supporting documentary evidence thereon.

(3) A regulated entity shall establish reasonable measures to ensure that employees involved in conducting or facilitating customer transactions are aware of suspicious transactions reporting procedures and consequences for the failure to report suspicious transactions.

Reporting on cash transactions.

41. A regulated entity shall report to the Centre any cash transaction equivalent to or exceeding ten thousand United States dollars or its equivalent in any other currency carried out by the entity whether or not the transaction appears to be suspicious.

42. (1) A regulated entity shall maintain a database of names and particulars of listed persons in the United Nations Sanctions List.

(2) A regulated entity shall, upon receipt from the Authority, keep updated the Sanctions List of various resolutions passed by the United Nations Security Council on combating terrorism and other relevant resolutions which require sanctions against individuals and entities.

(3) A regulated entity, upon receipt of the Sanctions List from the Authority, shall conduct regular checks on the names of new customers, as well as regular checks on the names of existing customers and potential customers, against the names in the Sanctions List.

(4) Where a regulated entity matches a name match on the Sanctions List with a name in its Sanction List database, it shall take reasonable and appropriate measures as required by the Prevention of Terrorism (Implementation of the United Nations Security Council Resolutions on Suppression of Terrorism) Regulations, 2013.

(5) A regulated entity shall ensure that the information contained in its Sanctions List database is up to date and easily accessible by its employees.

Compliance.

41. A regulated entity shall file with the Authority on a quarterly basis a report on compliance with these guidelines within thirty days after the end of the quarter.

42. (1) Where the Authority determines non-compliance with the provisions of these guidelines, it may take any intervention prescribed by the Insurance Act or any other relevant written law.

(2) Where the Authority determines that a regulated entity has not met the requirements of these guidelines, the Authority may impose any or all of the administrative sanctions specified in the Insurance Act to correct the situation including—

(a) directing the regulated entity to take appropriate remedial action;

(b) imposing additional reporting requirements and monitoring activities; and

(c) withdrawing or imposing conditions on the business license of the regulated entity based on the nature of the breach.

SCHEDULE

INDICATORS OF SUSPICIOUS TRANSACTIONS

1. A request by a customer to enter into an insurance contract(s) where the source of the funds is unclear or not consistent with the customer's apparent standing.
2. A sudden request for a significant purchase of a lump sum contract with an existing customer whose current contracts are minimal and of regular payments only.
3. A proposal which has no discernible purpose and a reluctance to divulge a "need" for making the investment.
4. A proposal to purchase and settle by cash.
5. A proposal to purchase by utilizing a cheque drawn from an account other than the personal account of the proposer.
6. The prospective client who does not wish to know about investment performance but does enquire on the early cancellation or surrender of the particular contract.
7. A customer establishes a large insurance policy and within a short time period cancels the policy, requests the return of the cash value payable to a third party.
8. Early termination of a product, especially in a loss.
9. A customer applies for an insurance policy relating to business outside the customer's normal pattern of business.
10. A customer requests for a purchase of insurance policy in an amount considered to be beyond his apparent need.
11. A customer attempts to use cash to complete a proposed transaction when this type of business transaction would normally be handled by cheques or other payment instruments.
12. A customer refuses, or is unwilling, to provide explanation of financial activity, or provides explanation assessed to be untrue.
13. A customer is reluctant to provide normal information when applying for an insurance policy, provides minimal or fictitious information or, provides information that is difficult or expensive for the institution to verify.
14. Delay in the provision of information to enable verification to be completed.
15. Opening accounts with the customer's address outside the local service area.
16. Opening accounts with names similar to other established business entities.
17. Attempting to open or operating accounts under a false name.
18. Any transaction involving an undisclosed party.
19. A transfer of the benefit of a product to an apparently unrelated third party.
20. A change of the designated beneficiaries (especially if this can be achieved without knowledge or consent of the insurer or the right to payment could be transferred simply by signing an endorsement on the policy).
21. Substitution, during the life of an insurance contract, of the ultimate beneficiary with a person without any apparent connection with the policy holder.
22. The customer accepts very unfavourable conditions unrelated to his health or age.
23. An atypical incidence of pre-payment of insurance premiums.

24. Insurance premiums have been paid in one currency and requests for claims to be paid in another currency.
25. Activity is incommensurate with that expected from the customer considering the information already known about the customer and the customer's previous financial activity. For individual customers, consider customer's age, occupation, residential address, general appearance, type and level of previous financial activity. For corporate customers, consider type and level of activity.
26. Any unusual employment of an intermediary in the course of some usual transaction or formal activity e.g. payment of claims or high commission to an unusual intermediary.
27. A customer appears to have policies with several institutions.
28. A customer wants to borrow the maximum cash value of a single premium policy, soon after paying for the policy.
29. The customer who is based in non-co-operative countries designated by the Financial Action Task Force from time to time or in countries where the production of drugs or drug trafficking may be prevalent.
30. The customer who is introduced by an overseas agent, affiliator or other company that is based in non-co-operating countries designated by the Financial Action Task Force from time to time or in countries where corruption or the production of drugs or drug trafficking may be prevalent.
31. A customer who is based in Kenya and is seeking a lump sum investment and offers to pay by a wire transaction or foreign currency.
32. Unexpected changes in employee characteristics including a lavish lifestyle or avoiding taking holidays.
33. Unexpected change in employee or agent performance, e.g. the sales person selling products has a remarkable or unexpected increase in performance.
34. Consistently high activity levels of single premium business far in excess of any average company expectation.
35. The use of an address which is not the client's permanent address, e.g. utilization of the salesman's office or home address for the dispatch of customer documentation.
36. Any other indicator as may be detected by the insurance institutions from time to time.

Dated the 13th February, 2020.

ABDIRAHIN H ABDI,
Chairman,
Insurance Regulatory Authority.

GODFREY K KIPTUM,
Commissioner of Insurance,
Insurance Regulatory Authority.