

Supplement No. 33

7th September, 2012

SUBSIDIARY LEGISLATION

to the Gazette of the United Republic of Tanzania No. 36 Vol 93 dated 7th September, 2012

Printed by the Government Printer, Dar es Salaam by Order of Government

GOVERNMENT NOTICE NO. 289 published on 07/09/2012

ANTI-MONEY LAUNDERING ACT

ARRANGEMENT OF REGULATIONS

PART I

PRELIMINARY PROVISIONS

Regulation *Title*

1. Citation.
2. Interpretation.

PART II

INFORMATION AND VERIFICATION OF CUSTOMER INFORMATION

(a) Citizens and Residents

3. Information concerning citizens and residents.
4. Verification of information concerning citizens and residents.

(b) Foreign Nationals

5. Information concerning foreign nationals.
6. Verification of information concerning foreign nationals.

(c) Entities

Anti-Money Laundering

G.N. No. 289 (contd.)

7. Information concerning local entities.
8. Verification of information concerning local entities.
9. Information concerning foreign entities.
10. Additional information concerning foreign entities.
11. Verification of information concerning foreign entities.

(d) Partnerships

12. Information concerning partnership.
13. Verification of information concerning partnerships.

(e) Trusts

14. Information concerning trusts.
15. Verification of information concerning trusts.
16. Death of individual or non existence of an individual, entity, partnership or trust.

PART III

RULES ON IDENTIFICATION

17. General rules on identification.
18. Reporting person to maintain correctness of particulars.

PART IV

REPORTING OF SUSPICIOUS TRANSACTIONS, CURRENCY TRANSACTIONS,
CROSS BORDER TRANSPORTATION OF CURRENCY AND
ELECTRONIC FUNDS TRANSFER

19. Manner of reporting.
20. Content of the report.
21. Establishment of procedures for recognizing and reporting suspicious transaction.
22. Reporting of suspicious transactions by reporting persons.
23. Information to be reported in respect of transactions.
24. Information to be reported concerning property associated with terrorist financing and related activities.

Anti-Money Laundering

G.N. No. 289 (contd.)

- 25. Information to be reported in respect of an account.
- 26. Information to be reported in respect of individuals or entities while conducting transactions.
- 27. Period for reporting.

PART V
CUSTOMER DUE DELIGENCE MEASURES

- 28. Application of customer due diligence.

PART VI
INTERNAL RULES

- 29. Internal rules concerning establishment and verification of identities.

PART VII
MISCELLANEOUS PROVISIONS

- 30. Records retention period.
- 31. Format and retrieval of records.
- 32. Access to information.
- 33. FIU to provide feedback.
- 34. Guidelines.
- 35. FIU to be availed with information.
- 36. FIU to maintain statistics.
- 37. Imposition of administrative sanctions.
- 38. Revocation.

—————
SCHEDULE
—————

ANTI-MONEY LAUNDERING ACT
(CAP 423)

REGULATIONS

—
(Made under section 29)
—

THE ANTI-MONEY LAUNDERING REGULATIONS, 2012

PART I
PRELIMINARY PROVISIONS

Citation 1. These Regulations may be cited as the Anti-Money Laundering Regulations, 2012.

Interpretation 2. In these Regulations unless the context otherwise requires-
Cap 423 "Act" means the Anti-Money Laundering Act;
 "AML" means an acronym of Anti Money Laundering;
 "AML/CFT" means an acronym of Anti Money Laundering and
 Combating the Financing of Terrorism;
 "business relationship" means an arrangement between a customer and a
 reporting person, where the purpose or effect of the arrangement
 is to facilitate the carrying out of transactions between the
 customer and the reporting person on a one-off, frequent,
 habitual or regular basis;
Cap 245 "BRELA" means an acronym for Business Registrations and Licensing
 Agency established under the Executive Agency Act;
 "CDD" means an acronym for Customer Due Diligence;
 "CIS" means an acronym for Collective Investment Schemes;
 "CMSA" means an acronym for Capital Market and Securities
 Authorities;
 "EDD" means an acronym for "Enhanced Due Diligence"
 "designated person" means a person appointed by a reporting person
 under section 18 of the Act;
 "FATF" means an acronym for the Financial Action Task Force;
 "FIU" means an acronym for Financial Intelligence Unit established

G.N. No. 289 (contd.)

- under section 4 of the Act;
- "Guidelines" means Guidelines issued by the FIU under section 6(f) of the Act;
- “KYC” means an acronym for Know Your Customer;
- “reporting person” has the meaning ascribed to it under section 3 of the Act;
- “STR” means an acronym for Suspicious Transaction Report;
- “TIRA” means an acronym for Tanzania Insurance Regulatory Authority.

PART II

INFORMATION AND VERIFICATION OF CUSTOMER INFORMATION

(a) *Citizens and Residents*

Information
on
concernin
g citizens
and
residents

3.-(1) Where a reporting person is dealing with an individual who is a citizen of, or resident in the United Republic he shall be required to obtain from such person the following information -

- (a) full names and residential address;
- (b) date and place of birth;
- (c) in case of a citizen, voters' registration card or national identity card or in the absence of such information, a passport, birth certificate or driving license;
- (d) in case of a resident, a passport, travel document, residence permit or driving license of that person;
- (e) an introductory letter from relevant authority such as employer or government official;
- (f) employee identity card with an introductory letter from employer ;
- (g) Tax Identification Number, if such a number has been issued to that person;
- (h) any or all of, telephone numbers, fax number, postal and e-mail address;
- (i) customer residential address including important landmarks close to the prospective customer's residence;
- (j) where the customer is a student-
- (k) an introductory letter from the customer's institution signed by the head of the institution or a representative of the head of institution;

Anti-Money Laundering

G.N. No. 289 (contd.)

- (l) the student's identity card;
 - (m) nature of business activity ;
 - (n) signature and thumb print;
 - (o) utility bills, where applicable.
- (2) In case a reporting person is aware or ought reasonably to be aware that the person referred to in sub-regulation (1) does not have the legal capacity to establish a business relationship or conclude a single transaction without the assistance of another person, the reporting person shall, in addition to obtaining the particulars referred to in sub regulation (1), obtain from the person rendering assistance-
- (a) full names and residential address;
 - (b) date and place of birth;
 - (c) Tax Identification Number, if such a number has been issued to that person;
 - (d) any or all of, telephone number, fax number, postal and email address;
 - (e) residential address including important landmarks close to his residence;
 - (f) nature of business relationship with the person he is helping; and
 - (g) signature and thumb print.
- (3) Where the reporting person is taking finger prints under these Regulations, he shall use ink and pad of such quality as to enable the capturing of thumb prints.
- (4) The thumb prints shall be taken in the following sequence-
- (a) where that person has both hands, right hand thumb shall be captured;
 - (b) where that persons has no right hand thumb, then the left hand thumb shall be captured;
 - (c) in case that person does not have both thumbs, then the next available finger shall be used, starting with the right pointing finger; and
 - (d) in case that person does not have fingers, the reporting person may take palm or toes print.
- (5) In case that person lacks both hands and feet, then an exceptional approval from the management of the reporting person shall be obtained after recording such situation.

Anti-Money Laundering

G.N. No. 289 (contd.)

(6) Where a reporting person is capable of using electronic form in capturing or storing finger prints, he shall be allowed.

(7) In determining the verification of identities under this regulation, the reporting person shall take into account Guidelines for the verification of identities applicable to the reporting person.

Verificati
on of
informati
on
concerni
ng
citizens
and
residents

4.-(1) A reporting person shall verify the full names, date and place of birth and Tax Identification Number of an individual referred to in regulation 3(1)(a), (b) or (c), or 3(2)(a), (b) or (c) by comparing these particulars with-

- (a) an identification document of that person; or
- (b) in the case where that person is, for a reason that is acceptable to the reporting person, unable to produce an identification document, another document issued to that person, which, taking into account any Guidelines concerning the verification of identities which may apply to that reporting person, is acceptable to the reporting person and bears-

- (i) a photograph of that person;
- (ii) that person's full names or initials and surname;
- (iii) that person's date and place of birth, and
- (c) any of these particulars with information which is obtained from any other independent source, if it is believed to be reasonably necessary taking into account any Guidelines concerning the verification of identities which may apply to that reporting person.

(2) A reporting person shall verify the Tax Identification Number referred to in regulation 3(1)(g) by comparing this number with a document issued by the Tanzania Revenue Authority bearing such a number and the name of the respective person.

(3) A reporting person shall verify the residential address referred to in regulation 3(1)(a) or 3(2)(a) by comparing these particulars with information which may reasonably be expected to achieve such verification and is obtained by practical means, taking into account any Guidelines concerning the verification of identities which may apply to that reporting person.

Anti-Money Laundering

G.N. No. 289 (contd.)

(p) Foreign nationals

Information concerning foreign nationals

5.-(1) A reporting person shall obtain from, or in respect of, an individual who is a citizen of another country and is not resident in the United Republic, that person's-

- (a) full names and residential address;
- (b) date and place of birth;
- (c) nationality;
- (d) passport;
- (e) visa;
- (f) Tax Identification Number, if such number has been issued to that person;
- (g) any or all of, telephone number, postal and email address; and
- (h) signature and thumb print.

(2) In case a reporting person is aware or ought reasonably to be aware that the person referred to in sub-regulation (1) does not have the legal capacity to establish a business relationship or conclude a single transaction without the assistance of another person, the reporting person shall, in addition to obtaining the particulars referred to in sub regulation (1), obtain from the person rendering assistance-

- (a) full names and residential address;
- (b) date and place of birth;
- (c) nationality;
- (d) passport;
- (e) Visa;
- (f) Tax Identification Number, if such number has been issued to that person;
- (g) signature and thumb print; and
- (h) any or all of, telephone number, postal and email address.

Verification of information concerning foreign nationals

6.-(1) A reporting person shall verify the particulars obtained in terms of regulation 5(1)(a), (b),(c), (d) and (e) or 5(2)(a),(b),(c), (d) and (e) from or in respect of an individual who is not a citizen or a resident in the United Republic by comparing those particulars with an identification document of that person.

(2) A reporting person shall verify the Tax Identification

G.N. No. 289 (contd.)

Number obtained in terms of regulation 5(1)(f) and 5(2)(f) from or in respect of an individual who is not a citizen or a resident in the United Republic, by comparing those particulars with a document issued by the Tanzania Revenue Authority bearing such a number.

(3) Notwithstanding the provisions of sub regulations (1) and (2), a reporting person may verify any of the particulars referred to in sub regulation (1) or (2) with information which is obtained from any other independent source, if it is believed to be reasonably necessary taking into account any Guidelines concerning the verification of identities which may apply to that reporting person.

(4) Where a reporting person doubts the authenticity of a non-resident's passport or identity document and the person is a prospective client, the reporting person shall seek advice from-

- (a) the embassy;
- (b) a consular officer of the prospective customer's country;
- (c) immigration office.

(5) Where a reporting person doubts the authenticity of a Visa, the reporting person shall seek advice from the immigration office.

(c) *Entities*

Informa-
tion
concerning
local
entities

7. A reporting person shall obtain from an individual acting or purporting to act on behalf of a local entity with which it is establishing a business relationship or concluding a single transaction-

- (a) the registered name of the entity;
- (b) the registered address of the entity;
- (c) the trade name under which the entity conducts business;
- (d) a copy of the latest audit report and accounts of the entity;
- (e) latest annual report duly certified by the Chief Executive Officer of BRELA;
- (f) the address from which the entity operates;
- (g) for multiple addresses-
 - (i) the address of the office seeking to establish a business relationship or to enter into a single transaction with the reporting person; and
 - (ii) the address of its head office;

G.N. No. 289 (contd.)

- (h) the full names, date and place of birth and Tax Identification Number, referred to in regulation 3(1)(a), (b) and (c) or full names, date and place of birth and name of the country referred to in regulation 5(1)(a), (b), (c), as may be applicable, concerning-
 - (i) the manager of the entity;
 - (ii) each individual who purports to be authorized to establish a business relationship or to enter into a transaction with the reporting person on behalf of the entity; and
 - (iii) the individual, partnership or trust holding 5% or more of the voting rights at a general meeting of the entity concerned.
- (i) the residential address and contact particulars of-
 - (i) the Directors;
 - (ii) each individual or entity holding 5% or more of the voting rights at a general meeting of the entity concerned; and
 - (iii) each individual who purports to be authorized to establish a business relationship or to enter into a transaction with reporting person on behalf of the entity.

Verification of information concerning local entities

- 8.** A reporting person shall verify the particulars obtained in respect of a local entity in terms of regulation 7 by comparing-
- (a) the registered name, registration number and registered address referred to in regulation 7(a), (b), (c) with the most recent Memorandum and Articles of Association and versions of the Certificate of Incorporation attested by BRELA;
 - (b) the trade name and business address referred to in regulation 7(d) and (f) with information which can reasonably be expected to achieve such verification and is obtained by practical means, taking into account any Guidelines concerning the verification of identities which may apply to that reporting person;
 - (c) the particulars referred to in regulation 7(g) and (h) with information obtained in accordance with regulation 4(1)

G.N. No. 289 (contd.)

- 6(1), 6(3), (a), (b) and (e) of these Regulations, as may be applicable;
- (d) resolution of the Board of Directors and power of Attorney granted to its manager, officer or employees to transact on its behalf;
- (e) the Tax Identification Number referred to in sub-regulation 7(h) with documents issued by the Tanzania Revenue Authority bearing such number;
- (f) extract from the Register issued by the Registrar of business names; and
- (g) any of these particulars with information which is obtained from any other independent source, if it is believed to be reasonably necessary taking into account any Guidelines concerning the verification of identities which may apply to that reporting person.

Informa-
tion
concerning
foreign
entities

9. A reporting person shall obtain from an individual acting or purporting to act on behalf of the foreign entity with which it is establishing a business relationship or concluding a single transaction-

- (a) the name under which it was incorporated;
- (b) the number under which it was incorporated;
- (c) the address where it is situated for purposes of its incorporation;
- (d) the name under which it conducts business in the country where it is incorporated;
- (e) the name under which it conducts business in the United Republic;
- (f) the address from which it operates in the country where it was incorporated, or if it operates from multiple addresses the address of its head office;
- (g) the address from which it operates in the United Republic, or if it operates from multiple addresses the address of the office seeking to establish a business relationship or enter into a single transaction with the reporting person;
- (h) the Tax Identification Number of the entity, if such number was issued to that entity;
- (i) Tanzania Investment Centre Certificate where applicable;

G.N. No. 289 (contd.)

- (j) Compliance Certificates issued by BRELA;
- (k) resolution of the Board of Directors and power of Attorney granted to its manager, officer or employees to transact on its behalf;
- (l) the full names, date and place of birth and Tax Identification Number referred to in regulation 3(1)(a), (b) and (g) or full names, date and place of birth and name of the country, referred to in regulation 5(1)(a), (b) and (f), as may be applicable, concerning
 - (i) the manager in respect of its affairs in the United Republic; and
 - (ii) each individual who purports to be authorized to establish a business relationship or to enter into a transaction with the reporting person on behalf of the foreign entity;
- (m) each individual, entity, partnership or trust holding 5% or more of the voting rights in the foreign entity.
- (n) any or all of telephone number, fax number, residential, postal and email address, of-
 - (i) the manager in respect of its affairs in the United Republic;
 - (ii) each individual or entity holding 5% or more of the voting rights in the entity; and
 - (iii) each individual who purports to be authorized to establish a business relationship or to enter into a transaction with the reporting person on behalf of the entity.

Additional
informa-
tion
concerning
foreign
entities

10.-(1) A reporting person who establishes a business relationship with a foreign entity, shall in addition to the information obtained in accordance with Regulation 9-

- (a) gather information about the foreign entity to understand the nature of its business to determine-
 - (i) the reputation of the entity;

Anti-Money Laundering

G.N. No. 289 (contd.)

- (ii) the quality of supervision of the entity;
 - (iii) whether the entity has been subject to money laundering or terrorist financing investigation or regulatory action; and
 - (b) assess the foreign entity's anti-money laundering and counter terrorist financing control to determine whether they are effective.
- (2) An officer of a reporting person shall obtain approval from senior management before establishing a business relationship with a foreign entity.

Verifica-
tion of
informa-
tion
concerning
foreign
entities

11.-(1) A reporting person shall verify the particulars obtained in respect of a foreign entity by comparing the particulars with an official document issued by an authority for recording the incorporation of entities in the country of incorporation of the foreign entity, as evidence of incorporation.

(2) Notwithstanding the provision of sub-regulation (1), the reporting person shall, when verifying information concerning the entity, take into account Guidelines concerning the verification of identities which may apply to that entity.

(j) Partnership

Informatio
n
concerning
partnership
s

12. A reporting person shall obtain from an individual acting or purporting to act on behalf of a partnership with which it is establishing a business relationship or concluding a single transaction-

- (a) the name of the partnership;
- (b) the full names, date and place of birth and Tax Identification Number, referred to in regulation 3(1)(a), (b) and (g), full names, date and place of birth, and name of the country referred to in regulation 5(1)(a), (b) and (f), registered name, registration number, registered address, trade name and business address referred to in regulation 7(a), (b), (c) and (d), as may be applicable, concerning-
 - (i) every partner;
 - (ii) the person who exercises executive control over

- the partnership; and
- (iii) each individual who purports to be authorized to establish a business relationship or to enter into a transaction with the reporting person on behalf of the partnership.

Verifica-
tion of
informa-
tion
concerning
partner-
ships

- 13.** A reporting person shall verify the particulars obtained in respect of partnership in terms of regulation 12 by comparing-
- (a) the name of the partnership referred to in regulation 12(a) with the partnership agreement in terms of which the partnership was formed;
 - (b) the particulars referred to in regulation 12(b) with information obtained in accordance with regulations 4(1), 6(1) and (3), 8(a), (b) and (e) or 15(1) (a) and (d) as may be applicable; and
 - (c) any of these particulars with information which is obtained from any other independent source, if it is believed to be reasonably necessary taking into account any Guidelines concerning the verification of identities which may apply to that reporting person.

(k) *Trusts*

Informa-
tion
concerning
trusts

- 14.** A reporting person shall obtain from an individual acting or purporting to act on behalf of a trust with which it is establishing a business relationship or concluding a single transaction-
- (a) the identifying name and number of the trust;
 - (b) the address of the Authority where the trust is registered;
 - (c) the Tax Identification Number of the trust, if such a number was issued to that trust;
 - (d) the full names, date and place of birth, referred to in regulating 3(1)(a) and (b), full names, date and place of birth and name of the country, referred to in regulation 5(1)(a), (b) and (c), registered name, registration number, registered address, trade name and business address referred to in regulation 7(a), (b), (c), (d) and (e);

G.N. No. 289 (contd.)

- (e) name referred to in regulation 12(a) as may be applicable, concerning-
 - (i) each trustee of the trust; and
 - (ii) each individual who purports to be authorized to establish a business relationship or to enter into a transaction with the reporting person on behalf of the trust;
- (f) the full names, date and place of birth, referred to in regulation 3(1)(a) and (b), full names, date and place of birth and name of the country, referred to in regulation 5(1)(a), (b) and (c), registered name, registration number, registered address, trade name and business address referred to in regulation 7(a), (b), (c), (d) and (e); names, numbers and addresses referred to in regulation 9(a), (b) and (c) name referred to in regulation 12(a) as may be applicable, concerning each beneficiary of the trust referred to by name in the trust deed or other founding instrument in terms of which the trust was created;
- (g) the full names, date and place of birth, referred to in regulation 3(1)(a) and (b), full names, date and place of birth and name of the country, referred to in regulation 5(1)(a), (b) and (c), registered name, registration number, registered address, trade name and business address referred to in regulation 7(a), (b), (c), (d) and (e); names, numbers and addresses referred to in regulation 9(a), (b) and (c) and name referred to in regulation 12(a) as may be applicable, concerning the founder of the trust;
- (h) the telephone number, fax number, residential postal and email address of-
 - (i) each trustee of the trust;
 - (ii) each individual who purports to be authorized to establish a business relationship or to enter into a transaction with the reporting person on behalf of the trust;
 - (iii) each beneficiary of the trust referred to by name in the trust deed or other founding instrument establishing the trust; and
 - (iv) the founder of the trust.

G.N. No. 289 (contd.)

Verifica-
tion of
informa-
tion
concerning
trusts

15. A reporting person shall verify the particulars obtained in respect of a trust in terms of regulation 14 by comparing-

- (a) the name and other particulars referred to in regulation 14(a) and (f) with the trust deed or other founding instruments establishing the trust and the particulars referred to in regulation 14(d), (e) or (f) with information obtained in accordance with regulation 4(1), 6(1) and (3), 8(a), (b) and (c) and 13(c) as may be applicable and –

Cap. 318

- (i) in the case of a trust created in the United Republic, the authorization given by the Registration, Insolvency and Trustees Agency in terms of Trustees Incorporation Act to each trustee of the trust to act in that capacity; or

- (ii) in the case of a trust created outside the United Republic, an official document which reflects these particulars issued by an authority in the country where the trust is created which administers or oversees laws relating to trusts in that country;

- (b) the address referred to in regulation 14(b) with the authorization given by the Authority to each trustee of the trust to act in that capacity;

- (c) the Tax Identification Number of the trust referred to in regulation 14(c) with a document issued by the Tanzania Revenue Authority bearing such a number; and

- (d) any of these particulars with information which is obtained from any other independent source, if it is believed to be reasonably necessary taking into account any Guidelines concerning the verification of identities which may apply to that reporting person.

Death of
individual
or non
existence
of an
individual,
entity,
partnership
or trust.

16. Where an individual, entity, partnership or trust referred to in this Part dies or ceases to exist, a reporting person shall verify the particulars referred to in this Part by comparing those particulars with information which can reasonably be expected to achieve such verification and is obtained by practical means, taking into account any Guidelines concerning the verification of identities which may apply to that reporting person.

PART III
RULES ON IDENTIFICATION

General
rules on
identificati
on

17. Each reporting person shall maintain identification procedures that-

- (a) require the satisfactory production of evidence of the identity of a person before a reporting person establishes a business relationship with that person;
- (b) take into account the suspicion of money laundering or the financing of terrorism where a prospective customer of the reporting person is not physically present during the identification process;
- (c) the business relationship or single transaction should not be continued where the reporting person is unable to obtain satisfactory evidence of the prospective customer's identity;
- (d) identify the third person who acts on behalf of the customer;
- (e) allow a reporting person to obtain information on the purpose and intended nature of a business relationship;
- (f) require a reporting person to conduct ongoing due diligence by scrutinizing transactions undertaken throughout the course of the business relationship to ensure that-
 - (i) the transactions being conducted are consistent with the reporting person's knowledge of the client;
 - (ii) the business and risk profile of the customer are contained; and
 - (iii) the customer's source of funds are investigated;
- (g) ensure that information collected under the customer due diligence process is updated.

Maintena-
nce of
correctness
of
particulars

18. A reporting person shall take reasonable steps, taking into account any Guidelines concerning the verification of identities which may apply to that reporting person in respect of an existing business relationship, to maintain the correctness of particulars as provided under these Regulations.

PART IV
REPORTING OF SUSPICIOUS TRANSACTIONS, CURRENCY
TRANSACTIONS, CROSS BORDER TRANSPORTATION OF
CURRENCY AND ELECTRONIC FUNDS TRANSFER

Manner of reporting

19. A report made under sections 4 (2), 17 and 23 of the Act shall be made in accordance with the format and in such manner as may be prescribed by the FIU in the Guidelines.

Content of the report

- 20.** A report under section 17 of the Act shall-
- (a) contain a full description of the suspicious transaction, including the reasons why it is deemed to be suspicious;
 - (b) contain action the reporting person has taken in connection with the suspicious transaction concerning which the report is made; and
 - (c) contain copies of supporting documents if available in respect of the suspicious transaction concerning which the report is made and the reasons referred to in paragraph (a).

Establishment of procedures for recognizing and reporting suspicious transaction

- 21.-(1)** A reporting person shall establish written internal reporting procedures which, in relation to its relevant business, shall-
- (a) enable all its directors or partners as the case may be, all other persons involved in its management and staff to know to whom they should report any knowledge or suspicion of money laundering and terrorist financing activities;
 - (b) designate a Money Laundering Reporting Officer to whom a report shall be made of any information or other matter which comes to the attention of the person handling that business and which in that person's opinion give rise to knowledge or suspicion that

another person is engaged in money laundering and terrorist financing;

- (c) ensure that there is a clear reporting chain under which suspicious money laundering and terrorist financing activities are passed to the Money Laundering Reporting Officer;
- (c) require the Money Laundering Reporting Officer to consider any report in the light of other relevant information available to him for the purpose of determining whether or not it gives rise to knowledge or suspicion of money laundering and terrorist financing;
- (d) ensure that the designated person has reasonable access to any other information which may be of assistance to him and which is available to the reporting person; and
- (e) require that the information or other matter contained in a report is disclosed promptly to the reporting person where the designated person knows or suspects that another person is engaged in money laundering and terrorist financing.

(2) The Money Laundering Reporting Officer appointed under sub regulation 1(b) shall be a senior officer to be able to liaise between the Management and other staff on matters related to money laundering and terrorist financing.

(3) A reporting person shall maintain a register of all reports made to the Money Laundering Reporting Officer in pursuance of sub-regulation (1)(f).

(4) The register maintained under sub-regulation (3) shall contain details of the date on which the report was made, the person who made the report, the amount and type of currencies involved and any other information that may help prove or clarify grounds of suspicion.

Reporting
of suspicious
transactions
by reporting
persons

22.-(1) A reporting person shall pay special attention to all complex, unusual or large business transactions, currency transaction reports, cross border currency reports and electronic funds transfer reports, whether completed or not and to all unusual patterns of transactions and to insignificant but periodic

Anti-Money Laundering

G.N. No. 289 (contd.)

transactions, which have no apparent economic or lawful purpose.

(2) Upon reasonable suspicion that the transaction described in sub-regulation (1) may constitute or be related to money laundering or terrorist financing, a reporting person shall promptly report the suspicious transaction to the FIU.

Information
to be
reported in
respect of
transactions

23. A report made under sections 4(2) and 17 of the Act, shall contain the following information -

- (a) date and time of the transaction, or, in case of a series of transactions the period over which the transactions were conducted;
- (b) type of funds or property involved;
- (c) amount or value of property involved;
- (d) currency in which the transaction was conducted;
- (e) method in which the transaction was conducted;
- (f) method in which the funds or property were disposed of;
- (g) amount disposed;
- (h) currency in which the funds were disposed of;
- (i) purpose of the transaction;
- (j) names of other institutions or person involved in the transaction;
- (k) bank account numbers in other institution involved in the transaction;
- (l) the name and identifying number of the branch or office where the transaction was conducted; and
- (m) any remarks, comments or explanation which the person conducting the transaction may have made or given in relation to the transaction.

G.N. No. 289 (contd.)

Information
to be
reported
concerning
property
associated
with
terrorist
financing
and related
activities

24.-(1) When a reporting person makes a report concerning property associated with terrorist financing and related activities under sections 4(2) and 17 of the Act, the report shall contain the following information-

- (a) full names of the owner or interested party to the property;
- (b) the identifying particulars of the owner or interested party to the property such as-
 - (i) in the case of natural person: passport number, voters registration card, national identity card, Tax Identification Number, identity number or registration number and any other particulars which can reasonably identify him
 - (ii) in the case of a legal person: Company registration number and certificate of incorporation;
- (c) the address of the owner or interested party to the property; and
- (d) occupation of the owner or interested party to the property.

(2) In respect of the property concerning which a report under sections 4 (2) and 17 of the Act is made, the report shall contain the following information -

- (a) type of property;
- (b) description of the property;
- (c) any identifying particulars concerning the property such as registration particulars, unique numbers or other particulars;
- (d) the estimated value of the property; and

Anti-Money Laundering

G.N. No. 289 (contd.)

(e) the physical address where the property is located.

Information
to be
reported in
respect of an
account

25. If a bank account is involved in the transaction concerning a report made under section 4(2) and 17 of the Act, the report shall contain the following information-

- (a) account number;
- (b) name and identifying number of the branch or office where the account is held;
- (c) type of account;
- (d) full names of each account holder;
- (e) address of the account holder which includes physical address;
- (f) date on which the account was opened;
- (g) status of the account;
- (h) date on which the account was closed and the name of the person who gave the instructions to close it;
- (i) any previous activity in the preceding six months which had been considered for reporting in connection with the account, whether the activity was reported or not; and
- (j) report the number of any previous reports made in connection with the account.

Information
to be
reported in
respect of
individuals
or entities
while
conducting
transactions

26. In respect of an individual or entity conducting a transaction or an individual or an entity on whose behalf the transaction is conducted, concerning which a report under sections 4(2) and 17 is made, the report shall contain the following information:

- (a) in the case of an individual-
 - (i) the person's full names;
 - (ii) the person's identifying number, if any;
 - (iii) the copy of identifying document from which

G.N. No. 289 (contd.)

- the particulars referred to in sub-paragraphs (i) and (ii) were obtained;
 - (iv) the person's country of residence;
 - (v) any or all of the person's residential address, telephone number, fax number, postal and email address; and
 - (vi) occupation;
- (b) in the case of an entity -
- (i) the entity's name and address;
 - (ii) the entity's identifying number, if it has such a number;
 - (iii) the type of business conducted by the entity;
 - (iv) the entity's country of origin;
 - (v) the names of individuals with authority to conduct the transactions on behalf of the entity.
- (c) in respect of an individual or other entity conducting a transaction on behalf of whom a transaction is made, a report under sections 4(2) and 17 shall contain the following information-
- (i) the person's full names and address;
 - (ii) the person's identifying number, if any;
 - (iii) the type of identifying document from which the particulars referred to in paragraphs (a) or (b) were obtained;
 - (iv) the person's country of residence;
 - (v) any or all of the person's residential address, telephone number, fax number, postal and email address; and
 - (vi) the person's occupation.

Period for reporting

27. A report made under sections 4(2) and 17 of the Act shall be submitted to the FIU as soon as possible but not later than twenty four hours after a reporting person has become aware or has knowledge of a suspicious transaction.

PART V
CUSTOMER DUE DILIGENCE MEASURES

Application
of customer
due diligence

28.-(1) Every reporting person shall apply Customer Due Diligence measures when-

- (a) establishing a business relationship;
- (b) carrying out an occasional transaction;
- (c) money laundering or terrorist financing is suspected;
or
- (d) veracity or adequacy of documents, data or information previously obtained for the purposes of identification or verification is doubted.

(2) A reporting person shall identify and verify the beneficial owners during the course of establishing a business relationship or when conducting transactions with its customers.

(3) A reporting person shall identify and verify the beneficial owners when conducting occasional transactions with its customers.

(5) Subject to sub-regulation (2) and (3), the reporting person shall undertake reasonable measures to verify the identity of the beneficial owner such that the reporting person is satisfied that it knows who the beneficial owner.

(6) A reporting person shall apply customer due diligence measures at other appropriate times to existing customers on a risk sensitivity basis.

(7) When dealing with entities, the reporting person shall undertake CDD measures to determine the natural persons that ultimately own or control the legal person or arrangement.

- (8) A reporting person shall-
- (a) determine the extent of customer due diligence measures on a risk sensitivity basis depending on the type of customer, business relationship, product or transaction; and
 - (b) be able to demonstrate to his supervisory authority that the extent of the measures is appropriate in view of the risks of money laundering and terrorist financing.

(9) Notwithstanding the provisions of this regulation, reporting persons whose requirements are stipulated in the

G.N. No. 289 (contd.)

Schedule to these Regulations, shall observe the customer due diligence as stipulated in the Schedule.

PART VI
INTERNAL RULES

Internal
rules
concerning
establishment
and
verification
of identities

29. -(1) The internal rules of a reporting person concerning the establishment and verification of identities shall-

- (a) provide for the necessary procedures which shall cause the required particulars concerning the identities of the parties to a business relationship or single transaction to be obtained on each occasion when a business relationship is established or when a single transaction is concluded;
- (b) provide for steps to be taken by staff members aimed at verifying particulars concerning the identities of the parties to a business relationship or single transaction;
- (c) provide for the responsibility of the management for compliance with the Act, these Regulations and the internal rules;
- (d) allocate responsibilities and accountability measures to ensure that staff duties concerning the establishment and verification of identities are complied with;
- (e) provide for disciplinary steps against the relevant staff members for non-compliance with the Act, these Regulations and the internal rules;
- (f) take into account any Guideline concerning the verification of identities which may apply to that reporting person;
- (g) provide for the necessary procedures to ensure that staff members of the reporting person obtain information of which record shall be kept on each occasion when a business relationship is established or a transaction is concluded;
- (h) provide for the necessary procedures to ensure that the accuracy and integrity of those records are

maintained for the entire period for which they shall be kept;

- (i) provide for the necessary procedures to ensure that there is unhindered access to information to authorized persons under the Act and these Regulations;
- (j) provide for the necessary procedures which shall cause suspicious transactions, currency transaction reports, cross border transportation of currency reports, electronic funds transfer reports to be reported to the FIU without delay;
- (k) provide for the necessary procedures to enable staff to recognize potential suspicious transactions, currency transactions, cross border transportation of currency, electronic funds transfers or series of transactions;
 - (1) allocate duties, responsibilities and accountability to staff in a manner that will ensure compliance with the Act and these Regulations.
 - (2) Where a reporting person doubts the authenticity of a non-resident's passport or identity document and the person is a prospective customer, the reporting person shall seek advice from-
 - (a) the embassy;
 - (b) a consular officer of the prospective customer's country;
 - (c) immigration office.
 - (3) Where a reporting person doubts the authenticity of a Visa, the reporting person shall seek advice from the immigration office.

**PART VII
MISCELLANEOUS PROVISIONS**

Records
retention
period

30.-(1) A reporting person shall retain records required by section 16 of the Act for a minimum period of ten years from the date-

- (a) when all activities relating to a transaction or a series of linked transactions were completed;
- (b) when the business relationship was formally ended;

G.N. No. 289 (contd.)

or

(c) where the business relationship was not formally ended but when the last transaction was carried out.

(2) where a reporting person is required by any enactment to release a record referred to in sub regulation (1) before the period of ten years lapses, the reporting person shall retain a copy of the record.

(3) Where a report has been made to the FIU pursuant to the provisions of the Act or the reporting person knows or believes that a matter is under investigation, that person shall without prejudice to sub-regulation (1), retain all relevant records for as long as may be required by the FIU.

(4) For the purpose of this regulation, the question as to what records may be relevant in the analysis process may be determined in accordance with the Guidelines.

Format and retrieval of records

31.-(1) A reporting person shall ensure that any records required to be maintained under these Regulations are retrievable without delay and they can be retrieved in legible format.

(2) A reporting person may rely on the records of a third party in respect of the details of payments and transactions by customers, provided that it is satisfied that the third party is willing and able to retain and, if asked to produce in legible form, copies of the records required.

Access to information

32.-(1). In carrying out its duties under section 6 of the Act, the FIU shall request in writing, any information from any reporting person, regulator or law enforcement agency.

(2) Any reporting person, regulator or law enforcement agency shall, immediately after receiving the request, under sub-regulation (1), provide such information.

(3) Where a reporting person, regulator or law enforcement agency fails to comply with the provision of sub-regulation (2), shall submit in writing reasons to FIU for such failure.

Anti-Money Laundering

G.N. No. 289 (contd.)

FIU to
provide
feedback

33. The FIU shall provide the reporting persons with feedback which includes-

- (a) acknowledgement of the receipt of suspicious transactions reports and results of investigation;
- (b) whether criminal proceedings have been instituted in court in relation to a submitted STR;
- (c) whether a report was found to relate to a legitimate transaction; and
- (d) information on the decision or results.

Guidelines

34. As required by section 6 of the Act, the FIU shall issue Guidelines related to -

- (a) the verification of customer identities;
- (b) reporting of suspicious transactions;
- (c) reporting currency transactions;
- (d) reporting electronic fund transfer;
- (e) reporting cross border currency transportation; and
- (f) any other obligations imposed on reporting persons under the Act.

FIU to be
availed with
information

35.-(1) Law Enforcement Agencies shall on timely basis provide the following information to FIU-

- (a) acknowledgment of the receipt of the disseminated reports;
- (b) updates of investigation; or
- (c) results of investigation undertaken.

(2) For the purposes of enabling the FIU maintain statistics on matters related to money laundering and terrorist financing, the Attorney General shall provide information to the FIU on the number of mutual legal assistance and extradition requests made or received and the status of the cases on money laundering and terrorist financing.

(3) The information requested under sub-regulation (2) shall include-

G.N. No. 289 (contd.)

- (a) nature of the request;
- (b) time the request was made;
- (c) time the response was received; and
- (d) refusal or granting of assistance requested;
- (e) the status of criminal proceedings instituted in relation to money laundering and the financing of terrorism;
- (f) number of cases related to money laundering and financing of terrorism including-
 - (i) outcome of the cases and the amount of money involved;
 - (ii) amount of property frozen, seized or confiscated.

FIU to
maintain
statistics

36.-(1) The FIU shall maintain comprehensive statistics on matters relevant for effective and efficient systems for combating money laundering and terrorist financing in the country.

- (2) The statistics under sub-regulation (1) shall include-
- (a) suspicious transaction reports received and intelligence disseminated;
 - (b) the reporting person or persons who made the report;
 - (c) breakdown of suspicious transactions on anti-money laundering and terrorist financing analyzed and disseminated by the FIU;
 - (d) reports filed on domestic or foreign currency transactions above the limit prescribed by the Minister;
 - (e) reports on cross border transportation of currency;
 - (f) reports on international electronic funds transfers;
 - (g) money laundering and terrorist financing analysis;
 - (h) the number of cases and the amounts of property frozen, seized or confiscated in relation to money laundering and terrorist financing;
 - (i) mutual legal assistance and extradition requests made or received in relation to money laundering and terrorist financing including -
 - (i) the nature of the request;

G.N. No. 289 (contd.)

- (ii) response times; and
- (iii) whether the assistance or request was granted or refused;
- (j) formal requests for assistance made by the FIU and whether they were granted or refused;
- (k) referrals made by the FIU to foreign authorities; and
- (l) formal requests for assistance made or received by reporting persons related to money laundering and terrorist financing including whether the request was granted or refused.

Imposition of administrative sanctions

37.-(1) The FIU or regulator may, upon being satisfied that a reporting person has failed to comply with the provisions of sections 15, 16, 17, and 18 of the Act, impose administrative sanctions.

(2) The FIU or regulator shall impose any of the following administrative sanctions-

- (a) warning or caution not to repeat the conduct which led to non-compliance referred to in sub-regulation (1);
- (b) a reprimand;
- (c) directive to take remedial action or to make specific arrangement to remedy the default;
- (d) restriction or suspension of certain business activities;
- (e) suspending a business license; or
- (f) suspension or removal from office any member of staff who cause or fail to comply.

(3) Before imposing an administrative sanction, the FIU or regulator shall give the reporting person notice in writing-

- (a) of the nature of the alleged non-compliance;
- (b) of the intention to impose administrative sanction; and
- (c) of the amount or particular of the intended administrative sanction.

(4) The reporting person may, in writing, within a period specified in the notice, make representations as to why the administrative sanctions should not be imposed.

(5) Subject to sub-regulation (2) the FIU or regulator

Anti-Money Laundering

G.N. No. 289 (contd.)

when determining an appropriate administrative sanction, shall consider the following-

- (a) the nature, duration, seriousness and extent of the default;
 - (b) whether the reporting person has previously failed to comply with any written laws; and
 - (c) any remedial steps taken against by the reporting person to prevent a recurrence.
- (6) Where the FIU or regulator has imposed sanctions under sub regulation (2) paragraphs (a), (b) and (c) and reporting person fails comply with such sanctions, the FIU or regulator shall impose a fine not exceeding five million shillings per day for which a default is committed.

Revocation
GN No. 195
of 2007

38. The Anti-Money Laundering Regulations, 2007 is hereby revoked.

—
SCHEDULE
—

(Made under regulation 28 (7))
—

A. VERIFICATION OF CUSTOMERS' IDENTITIES

(a) For natural persons

1. In case a person is unable to produce an official identity document, reporting persons shall be satisfied that the customer has an acceptable reason for being unable to produce an official identity document.
2. The reason(s) provided under paragraph 1 shall be noted in the records of the reporting person(s).
3. Reporting persons shall confirm the permanent address using such things as utility bills, a letter from a public authority or embassy or consular office, recent lease or rental agreement or any other document which bear such information and which is obtained from any credible independent source.
4. Reporting persons shall contact the customer by telephone, letter or by e-mail to confirm the information supplied before and after the relationship has been established. Things like a disconnected phone, returned mail, or incorrect e-mail address should warrant further investigation.
5. Reporting persons shall confirm the validity of the official documentation provided through certification by an authorised person (e.g. government official, public notary, embassy.).
6. Reporting persons shall apply equally effective customer identification procedures for non-face-to-face customers as for those available for interview and must take reasonable steps to confirm the existence of the customer and verify the identity of the person involved and there must be specific and adequate arrangements to mitigate the higher risk by taking such measures as:
 - (a) certification of documents presented;
 - (b) requisition of additional documents to complement those that are required for face to face customers;
 - (c) independent contact with customer by the reporting persons; and
 - (d) third party introduction.

(b) For entities' identities (corporate, partnerships, associations or clubs, sole proprietorships and trusts)

Anti-Money Laundering

G.N. No. 289 (contd.)

1. For established corporate entities, reporting persons shall review a copy of the latest periodical reports and audited accounts, if available.
2. Reporting persons shall communicate with BRELA and other registering authorities on the authenticity of registration certificates and communicating with Tanzania Investment Centre, if applicable, for verification of necessary documents.
3. Reporting persons shall undertake an entity search or other enquiries to ensure that the entity has not been, or is not in the process of being, dissolved, struck off, wound up or terminated.
4. Reporting persons shall utilize an independent information verification process, including accessing public and private databases.
5. Reporting persons shall, in addition to the above-
 - (a) obtain prior bank references;
 - (b) gather information about the foreign entity for the purpose of determining-
 - (i) the reputation of the foreign entity;
 - (ii) whether the foreign entity has been subject to money laundering or terrorist financing investigation or regulatory action; and
 - (iii) whether the foreign entity's anti-money laundering and counter terrorist financing controls are effective.
6. For charities, clubs and societies, reporting persons shall take reasonable steps to identify and verify at least two signatories, in line with natural person identification, along with the entity itself the principals to be identified shall be those persons exercising control or significant influence over the organisation's assets. This will include members of a governing body or committee, the President, any board member, the treasurer, and all signatories. Such identity verification shall be in line with natural person verification procedures.
7. Where Mutual or Friendly societies, Non-Governmental Organizations, Political parties, Cooperatives and societies are involved, reporting persons shall identify the persons exercising control or significant influence over the organisation's assets. This will include board members plus executives and account signatories. Such identity verification shall be in line with natural persons verification procedures.

(c) For other persons such as organs of state including government ministries or departments, embassies and parastatals

1. Reporting persons shall verify the identity of all their customers, including organ of state such as government ministries or departments, embassies and parastatals.
2. Reporting persons shall verify the identity of organs of state which are incorporated as companies to conduct business.
3. Reporting persons shall identify other organs with legal person's identity by

Anti-Money Laundering

G.N. No. 289 (contd.)

identifying representatives or persons acting on behalf of an organ of state by obtaining and verifying their full names, dates of birth, identity numbers, and photographs. Information concerning the contact particulars of such persons shall be obtained and verification done in line with these Regulations.

(d) for third party or agent identities verification

1. Where a client is acting on behalf of another person, the reporting person shall establish and verify the identity of that other person and the client's authority to establish the business relationship or conclude the transaction on behalf of that person.
2. Reporting persons shall verify the information obtained by comparing the particulars of the person in line with these Regulations.
3. Reporting persons on verifying the authority of a third party acting on behalf of another person when establishing a relationship, shall confirm the identity of that person using such documents as power of attorney, mandate resolution duly executed by authorised signatories or a court order authorising the third party to conduct business on behalf of another person.
4. Reporting persons shall take reasonable steps to verify the identity and reputation of any agent transacting on behalf of a customer, if he is a natural person, shall be identified like a natural person and, if it is an entity, shall be identified like entities as provided for in these Regulations.

(e) For ongoing customer details maintenance

1. Reporting persons shall take reasonable steps, concerning verification of customer identities in respect to existing business relationship, to maintain the correctness of particulars that are susceptible to change.
2. Reporting persons shall-
 - (a) apply Know Your Customer (KYC) procedures to existing customers on the basis of materiality and risk and conduct due diligence reviews of such existing relationships as appropriate;
 - (b) undertake regular reviews of existing customer records; and
 - (c) if a reporting person becomes aware at anytime that it lacks sufficient information about an existing customer, the reporting person shall take steps to obtain all relevant KYC information as quickly as possible.

B. BANK OF TANZANIA

1. The Bank of Tanzania shall, during onsite examination satisfy itself that banks and financial institutions have sound Know Your Customer (KYC), Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD) for more risky customers and transaction policies and procedures.
2. The Bank of Tanzania shall, during onsite examination satisfy itself that banks and financial institutions retain records pertaining to customer identification and transactions as required by the Act, these Regulations and Guidelines.

G.N. No. 289 (contd.)

3. The Bank of Tanzania shall during onsite examination satisfy itself that banks and financial institutions verify identities of the customers they deal with in line with the provisions of the Act, these Regulations and Guidelines.

C. BANKS OR FINANCIAL INSTITUTIONS

1. The bank or financial institution shall have sound Know Your Customer (KYC) policies and procedures.
2. Key elements in the design of KYC programs shall include customer acceptance policy, customer identification, ongoing monitoring of high-risk accounts and risk management.
3. The bank or financial institution shall not keep anonymous accounts or accounts in fictitious names.
4. The bank or financial institution shall undertake customer due diligence measures, including identifying and verifying the identity of their customers, when:
 - (a) establishing business relations;
 - (b) carrying out occasional transactions;
 - (c) there is a suspicion of money laundering or terrorist financing;
 - (d) there are doubts about the veracity or adequacy of previously obtained customer identification information.
5. The bank or financial institution shall refuse to enter into, or continue, a correspondent banking relationship with shell banks and shall also guard against establishing relations with respondent foreign bank or financial institutions that permit their accounts to be used by shell banks.
6. The bank or financial institution shall pay special attention to any money laundering threats that may arise from new or developing technologies that might favour anonymity, and take measures, if needed, to prevent their use in money laundering schemes. In particular, bank or financial institutions shall have policies and procedures in place to address any specific risks associated with non face-to-face business relationships or transactions.
7. The bank or financial institution shall pay special attention to all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or viable lawful purpose. The background and purpose of such transactions should, as far as possible, be examined, the findings established, put in writing, and made available to help competent authorities.
8. The Customer Due Diligence measures to be taken includes the following:
 - (a) identifying the customer and verifying customer's identity using reliable, independent source documents, data or information;
 - (b) identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner such that the banking institution is satisfied that it knows who the beneficial owner is;
 - (c) obtaining information on the purpose and intended nature of the business relationship;
 - (d) conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, including the source of funds.

Anti-Money Laundering

G.N. No. 289 (contd.)

9. The bank or financial institution shall apply each of the CDD measures pointed out under paragraph 8, but may determine the extent of such measures on a risk sensitive basis depending on the type of customer, business relationship or transaction. The measures that are taken should be consistent with any Guidelines issued by competent authorities. For higher risk categories, institutions should perform enhanced due diligence.
10. The bank or financial institution shall verify identities of the customers they deal with in line with the provisions of the Act, these Regulations and Guidelines.

The bank or financial institutions shall verify the identities of customers and beneficial owners before or during the course of establishing a business relationship or conducting transactions for walk in customers.
11. Where the institution is unable to verify the identity as provided under paragraphs 10 and 11, it shall not open the account, commence business relations or conclude the transaction; or it shall terminate the business relationship; and file a suspicious activity report in relation to the customer.
12. The bank or financial institution shall, in relation to politically exposed persons (as defined in the Act), in addition to performing normal due diligence measures-
 - (a) have appropriate risk management systems to determine whether the customer is a politically exposed person;
 - (b) obtain senior management approval for establishing business relationships with such customers;
 - (c) take reasonable measures to establish the source of wealth and source of funds;
 - (d) conduct enhanced ongoing monitoring of the business relationship.
13. In relation to cross-border correspondent banking and other similar relationships, in addition to performing normal due diligence measures, bank or financial institutions shall-
 - (a) gather sufficient information about a respondent institution to understand fully the nature of the respondent's business and to determine from publicly available information the reputation of the institution and the quality of supervision, including whether it has been subject to a money laundering or terrorist financing investigation or regulatory action;
 - (b) assess the respondent institution's anti-money laundering and terrorist financing controls;
 - (c) obtain approval from senior management before establishing new correspondent relationships;
 - (d) with respect to "payable-through accounts", be satisfied that the respondent bank has verified the identity of and performed on-going due diligence on the customers having direct access to accounts of the correspondent and that it is able to provide relevant customer identification data upon request to the correspondent bank.
14. The bank or financial institution shall retain records concerning customer identification and transaction.
15. The records prepared and maintained by any bank or financial institution on its customer relationships and transactions shall ensure that-
 - (a) requirements of legislation are fully met;

Anti-Money Laundering

G.N. No. 289 (contd.)

- (b) competent third parties will be able to assess the institution's observance of anti-money laundering and anti-terrorist financing policies and procedures;
 - (c) any transactions effected via the institution can be reconstructed; and
 - (d) the institution can satisfy enquiries from the appropriate authorities.
16. The bank or financial institution shall retain records for at least ten years as provided for under these Regulations whereby; retention may be by way of original documents, stored on hard copy files, microfiche, and computer disk or in other electronic form.
17. The records referred under paragraph 17 shall be sufficient to permit reconstruction of individual transactions including the date, amounts and types of currency involved so as to provide, if necessary, evidence for prosecution of criminal activity.
18. The bank or financial institution shall keep records on the identification data obtained through the customer due diligence process such as copies or records of official identification documents like passports, identity cards, driving licenses or similar documents, account files and business correspondence for at least ten years after the business relationship is ended.

D. INSURERS

1. No insurer shall deal with any person on an anonymous basis or any person using a fictitious name.
2. An insurer shall perform CDD measures when –
 - (a) the insurer establishes business relations with any customer;
 - (b) there is a suspicion of money laundering or terrorist financing; or
 - (c) the insurer has doubts about the veracity or adequacy of any information previously obtained.
3. An insurer shall identify each customer who applies to the insurer to establish business relations.
4. For the purpose of paragraph 3, an insurer shall obtain and record information of the customer in accordance with the Act, including but not limited to the following:
 - (a) full name, including any aliases;
 - (b) unique identification number such as an identity card number, birth certificate number, voters registration card number, driving license number, national ID number, number on introduction letter from the local government executive, passport number or where the customer is not a natural person, the incorporation number or business registration number;
 - (c) existing residential address, registered or business address as may be appropriate and contact telephone number(s);
 - (d) date of birth, incorporation or registration as may be appropriate; and
 - (e) nationality or place of incorporation or registration as may be appropriate.
5. Where the customer is a company, the insurer shall, apart from identifying the customer, also identify the directors of the company.

Anti-Money Laundering

G.N. No. 289 (contd.)

6. Where the customer is a partnership or a limited liability partnership, the insurer shall, apart from identifying the customer, also identify the partners.
7. Where the customer is any other body corporate or unincorporate, the insurer shall, apart from identifying the customer, also identify the persons having executive authority in that body corporate or unincorporate.
8. An insurer shall verify the identity of the customer using reliable, independent sources.
9. An insurer shall retain copies of all reference documents used to verify the identity of the customer.
10. An insurer shall inquire if there exists any beneficial owner in relation to a customer. "Beneficial owner", in relation to a customer of an insurer, means the natural person who ultimately owns or controls a customer or the person on whose behalf a transaction is being conducted and includes the person who exercises ultimate effective control over a body corporate or unincorporate.
11. Where there is one or more beneficial owners in relation to a customer, the insurer shall take reasonable measures to obtain information sufficient to identify and verify the identity of the beneficial owner(s).
12. Where the customer is not a natural person, the insurer shall take reasonable measures to understand the ownership and structure of the customer.
13. An insurer shall not be required to inquire if there exists any beneficial owner in relation to a customer that is-
 - (a) a Tanzanian Government entity;
 - (b) a foreign Government entity, provided it is not sanctioned or blacklisted by the international community such as the United Nations and FATF;
 - (c) an entity listed on the stock exchange in Tanzania;
 - (d) an entity listed on a stock exchange outside of Tanzania that is subject to adequate regulatory disclosure requirements (referred regulator should be a registered member of any International Association of Regulators);
 - (e) a bank or financial institution supervised by the Bank of Tanzania, the CMSA or the TIRA;
 - (f) a bank or financial institution incorporated or established outside Tanzania that is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF;
 - (g) Life insurance policies where the annual premium is not more than TZS 1,500,000 or EURO/USD 1000 or a single premium of no more than TZS 4,000,000 or EURO/USD 2500;
 - (h) Insurance policies for pension schemes if there is no surrender clause and the policy cannot be used as collateral; or
 - (i) A pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest under the scheme;
Unless the insurer suspects that the transaction is connected with money laundering or terrorist financing.
14. For the purposes of items (d) and (f) of paragraph 13, an insurer shall document the basis for its determination that the requirements in those paragraphs have been duly met.

Anti-Money Laundering

G.N. No. 289 (contd.)

15. Where a customer appoints one or more natural persons to act on his behalf in establishing business relations with the insurer or the customer is not a natural person, an insurer shall-
 - (a) identify the natural persons that act or are appointed to act on behalf of the customer, as if such persons were themselves customers;
 - (b) verify the identity of these persons using reliable, independent sources; and
 - (c) retain copies of all reference documents used to verify the identity of these persons.
16. In the case of private trusts, an insurer shall verify the authorization given to each trustee of the relevant trust.
17. An insurer shall verify the due authority of such person to act on behalf of the customer, by obtaining, including but not limited to, the following-
 - (a) the appropriate documentary evidence that the customer has appointed the persons to act on its behalf, and
 - (b) the specimen signatures of the persons appointed.
18. Where the customer is a Tanzanian government entity, the insurer shall only be required to obtain such information as may be required to confirm that the customer is a Tanzanian government entity as indicated.
19. Where the payee of the insurance policy is not a customer, an insurer shall identify the payee and verify his identity before making any of the following types of payment-
 - (a) payment of the sum assured (or part thereof) upon the occurrence of the risk insured against in accordance with the policy;
 - (b) payment of the surrender value of the insurance policy;
 - (c) refund of premium upon the avoidance, cancellation and/or termination of any insurance policy; or
 - (d) refund of any other payment made in relation to any insurance policy.
20. An insurer shall obtain, from the customer, when processing the application to establish business relations, information as to the purpose and intended nature of business relations.
21. An insurer shall perform CDD measures as may be appropriate to its existing customers having regard to its own assessment of materiality and risk.
22. When an insurer ("acquiring insurer") acquires, either in whole or in part, the business of another financial institution (whether in Tanzania or elsewhere), the acquiring insurer shall perform CDD measures on customers acquired with the business at the time of acquisition except where the acquiring insurer has:
 - (a) acquired at the same time all corresponding customer records (including customer identification information) and has no doubt or concerns about the veracity or adequacy of the information so acquired; and
 - (b) conducted due diligence enquiries that have not raised any doubt on the part of the acquiring insurer as to the adequacy of AML/CFT measures previously adopted in relation to the business or part thereof now acquired by the acquiring insurer.
23. In the case of a joint account, an insurer shall perform CDD measures on all of the joint account holders as if each of them were individually customers of the insurer.
24. An insurer that undertakes any transaction with a non-policy holder shall-

Anti-Money Laundering

G.N. No. 289 (contd.)

- (a) establish and verify the identity of the customer as if the customer had applied to the insurer to establish business relations; and
 - (b) record adequate details of the transaction so as to permit the reconstruction of the transaction, including the nature and date of the transaction, the type and amount of currency involved, the value date, and the details of the payee.

- 25. An insurer shall complete verification of the identity of the customer and beneficial owner-
 - (a) before the insurer establishes business relations; or
 - (b) before the insurer undertakes any transaction for a customer, where the customer does not have business relations with the insurer.

- 26. An insurer may establish business relations with a customer before completing the verification of the identity of the customer and beneficial owner if:
 - (a) the deferral of completion of the verification of the identity of the customer and beneficial owner is essential in order not to interrupt the normal conduct of business operations; and
 - (b) the risks of money laundering and terrorist financing can be effectively managed by the insurer,

in all cases, identification and verification should occur at or before the time of payout or the time when the beneficiary intends to exercise vested rights under the policy.

- 27. Where the insurer establishes business relations before verification of the identity of the customer or beneficial owner, the insurer shall complete such verification as soon as is reasonably practicable.

- 28. Where the insurer is unable to complete CDD measures, it shall terminate the business relationship and consider if the circumstances are suspicious so as to warrant the filing of a suspicious transaction report.

- 29. An insurer shall, in relation to politically exposed persons as defined in the Act, perform enhanced CDD measures in addition to normal CDD measures, including but not limited to the following-
 - (a) implement appropriate internal policies, procedures and risk management systems to determine if a customer or beneficial owner is a politically exposed person;
 - (b) obtain approval from the insurer's senior management to establish or continue business relations where the customer or beneficial owner is a politically exposed person or subsequently found to be or subsequently becomes a politically exposed person;
 - (c) take reasonable measures to establish the source of wealth and source of funds of the customer or beneficial owner; and
 - (d) conduct, during the course of business relations, enhanced monitoring of business relations with the customer.

- 30. An insurer shall perform enhanced CDD measures in referred to in paragraph 29 for other categories of customers, business relations or transactions as the insurer may assess to prevent a higher risk for money laundering and terrorist financing.

- 31. An insurer shall give particular attention to business relations and transactions with

Anti-Money Laundering

G.N. No. 289 (contd.)

- any person from or in countries and jurisdictions known to have inadequate AML/CFT measures, as determined by the insurer for itself or notified to insurers generally by the FIU or other foreign regulatory authorities.
32. An insurer shall put in place policies and procedures to address any specific risks associated with the use of new technologies and non-face-to-face business relations or transactions.
 33. An insurer shall implement the policies and procedures referred to in paragraph 31 when establishing customer relationships and when conducting ongoing due diligence.
 34. Where there is no face-to-face contact, the insurer shall carry out CDD measures that are as stringent as those that would be required to be performed if there were face-to-face contact.
 35. An insurer may rely on an intermediary to perform CDD measures in accordance with the Act and these Regulations if the following requirements are met-
 - (a) the insurer is satisfied that the intermediary it intends to rely upon is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF, and has adequate measures in place to comply with those requirements;
 - (b) the intermediary is not one on which insurers have been specifically precluded by relevant Tanzanian authorities from relying;
 - (c) the intermediary is able and willing to provide, without delay, upon the insurer's request, any document obtained by the intermediary which the insurer would be required or would want to obtain; and
 - (d) the intermediary has capacity in terms of competent staff and resources to carry out CDD.
 36. No insurer shall rely on an intermediary to conduct ongoing monitoring of customers.
 37. Where an insurer relies on an intermediary to perform the CDD measures, insurer shall:
 - (a) document the basis for its satisfaction that the requirements in item (a) of paragraph 35 have been met, and
 - (b) immediately obtain from the intermediary the information relating to CDD measures obtained by the intermediary.
 38. For the avoidance of doubt, notwithstanding the reliance upon an intermediary, the insurer shall remain responsible for its AML/CFT obligations as required under the Act, these Regulations and Guidelines.
 39. Every insurer shall prepare, maintain and retain documentation on all its business relations, transactions.
 40. An insurer shall, when setting its record retention policies and performing its internal procedures, comply with the following document retention periods-
 - (a) a period of at least ten years following the termination of business relation for customer identification document, and other documents relating to the establishment of business relations, as well as account files and business correspondence; and

Anti-Money Laundering

G.N. No. 289 (contd.)

- (b) a period of ten years following the completion of transaction for records relating to a transaction, including any information needed to explain and reconstruct the transaction.
- 41. An insurer shall retain records pertaining to a matter which is under investigation or which has been the subject of a suspicious transaction report (STR) for such longer period as may be necessary in accordance with any request or order from relevant competent authorities in Tanzania.
- 42. An insurer shall monitor on an ongoing basis, its business relations with customers.
- 43. An insurer shall, during the course of business relations, observe the conduct of the customer's policy and scrutinize transactions undertaken to ensure that the transactions are consistent with the insurer's knowledge of the customer, its business and risk profile and where appropriate, the source of funds.
- 44. An insurer shall pay special attention to all complex or unusually large transactions or unusual patterns of transactions that have no apparent or visible economic or lawful purpose.
- 45. An insurer shall take reasonable steps to inquire into the background and purpose of the transactions in paragraph 44 and document such information and its findings.
- 46. The records referred to under paragraph 45, shall be kept for at least ten years with a view to making this information available to the relevant competent authorities should the need arise.

E. CAPITAL MARKET AND SECURITIES AUTHORITY LICENSEES

- 1. No CMSA licensee shall deal with any person on an anonymous basis or any person using a fictitious name.
- 2. A CMSA licensee shall perform CDD measures when –
 - (a) the CMSA licensee establishes business relations with any customer;
 - (b) there is a suspicion of money laundering or terrorist financing, notwithstanding that the CMSA licensee would otherwise not be required by these Regulations to perform CDD measures; or
 - (c) the CMSA licensee has doubts about the veracity or adequacy of any information previously obtained.
- 3. A CMSA licensee shall identify each customer who applies to the CMSA licensee to establish business relations.
- 4. For the purpose of paragraph 3, CMSA licensee shall obtain and record information of the customer in accordance with the provisions of the Act, including but not limited to the following:
 - (a) full name, including any aliases;
 - (b) unique identification number such as an identity card number, birth certificate number, voter registration card number or passport number, or where the customer is not a natural person, the incorporation number or business registration number;
 - (c) existing residential address, registered or business address (as may be appropriate) and contact telephone number(s);
 - (d) date of birth, incorporation or registration (as may be appropriate); and
 - (e) nationality or place of incorporation or registration (as appropriate).

Anti-Money Laundering

G.N. No. 289 (contd.)

5. Where the customer is a company, the CMSA licensee shall, apart from identifying the customer, also identify the directors of the company.
6. Where the customer is a partnership or a limited liability partnership, the CMSA licensee shall, apart from identifying the customer, also identify the partners.
7. Where the customer is any other body corporate or unincorporate, the CMSA licensee shall, apart from identifying the customer, also identify the persons having executive authority in that body corporate or unincorporate.
8. A CMSA licensee shall verify the identity of the customer using reliable, independent sources.
9. A CMSA licensee shall retain copies of all reference documents used to verify the identity of the customer.
10. A CMSA licensee shall inquire if there exists any beneficial owner in relation to a customer. "Beneficial owner", in relation to a customer of a CMSA licensee, means the natural person who makes final decisions, ultimately controls a customer or the person on whose behalf a transaction is being conducted. This includes the person who exercises ultimate effective control over a body corporate or unincorporates.
11. Where there is one or more beneficial owners in relation to a customer, the CMSA licensee shall take reasonable measures to obtain information sufficient to identify and verify the identity of the beneficial owner(s).
12. Where the customer is not a natural person, the CMSA licensee shall take reasonable measures to understand the ownership and structure of the customer.
13. A CMSA licensee shall not be required to inquire if there exists any beneficial owner in relation to a customer that is –
 - (a) a Tanzanian Government entity;
 - (b) a foreign government entity, provided it is not sanctioned or blacklisted by the international community such as the United Nations or FATF;
 - (c) an entity listed on the stock exchange in Tanzania;
 - (d) an entity listed on a stock exchange outside of Tanzania that is subject to adequate regulatory disclosure requirements;
 - (e) a bank or financial institution supervised by the Bank of Tanzania, CMSA or TIRA;
 - (f) a bank or financial institution incorporated or established outside Tanzania that is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF;
 - (g) A pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest under the scheme,
unless the CMSA licensee suspects that the transaction is connected with money laundering or terrorist financing.
14. For the purposes of items (d) and (f) of paragraph 13, a CMSA licensee shall document the basis for its determination that the requirements in those paragraphs have been duly met.
15. Where a customer appoints one or more natural persons to act on his behalf in establishing business relations with the CMSA licensee or the customer is not a natural person, a CMSA licensee shall-
 - (a) identify the natural persons that act or are appointed to act on behalf of the

Anti-Money Laundering

G.N. No. 289 (contd.)

- customer, as if such persons were themselves customers;
 - (b) verify the identity of these persons using reliable, independent sources; and
 - (c) retain copies of all reference documents used to verify the identity of these persons.
16. In the case of private trusts, a CMSA licensee shall verify the authorization given to each trustee of the relevant trust.
17. A CMSA licensee shall verify the due authority of such person to act on behalf of the customer, by obtaining, including but not limited to, the following-
- (a) the appropriate documentary evidence that the customer has appointed the persons to act on its behalf; and
 - (b) the specimen signatures of the persons appointed.
18. Where the customer is a Tanzanian government entity, the CMSA licensee shall only be required to obtain such information as may be required to confirm that the customer is a Tanzanian government entity as indicated.
19. When a CMSA licensee (“acquiring CMSA licensee”) acquires, either in whole or in part, the business of another financial institution (whether in Tanzania or elsewhere), the acquiring CMSA licensee shall perform CDD measures on customers acquired with the business at the time of acquisition except where the acquiring CMSA licensee has:
- (a) acquired at the same time all corresponding customer records (including customer identification information) and has no doubt or concerns about the veracity or adequacy of the information so acquired; and
 - (b) conducted due diligence enquiries that have not raised any doubt on the part of the acquiring CMSA licensee as to the adequacy of AML/CFT measures previously adopted in relation to the business or part thereof now acquired by the acquiring CMSA licensee.
20. A CMSA licensee shall obtain, from the customer, when processing the application to establish business relations, information as to the purpose and intended nature of business relations.
21. Subject to paragraph 20, a CMSA licensee shall complete verification of the identity of the customer and beneficial owner:
- (a) before the CMSA licensee establishes business relations; or
 - (b) before the CMSA licensee undertakes any transaction for a customer, where the customer does not have business relations with the CMSA licensee.
22. A CMSA licensee may establish business relations with a customer before completing the verification of the identity of the customer and beneficial owner if -
- (a) the deferral of completion of the verification of the identity of the customer and beneficial owner is essential in order not to interrupt the normal conduct of business operations, and
 - (b) the risks of money laundering and terrorist financing can be effectively managed by the CMSA licensee.
23. Where the CMSA licensee establishes business relations before verification of the identity of the customer or beneficial owner, the CMSA shall adopt risk management procedures concerning the conditions under which the establishment

Anti-Money Laundering

G.N. No. 289 (contd.)

- of business relations before verification of the identity may occur.
24. The risk management procedures under paragraph 23 shall include measures such as a limitation of the number, types and/or amount of transactions that can be performed and the monitoring of large or complex transactions being carried out outside the expected norms for that type of relationship.
 25. The CMSA licensee shall complete the verification procedures under paragraph 23 as soon as is reasonably practicable.
 26. The CMSA licensee shall be ready to explain to competent authorities why the deferral of completion of the verification of the identity of the customer and beneficial owner is essential in order not to interrupt the normal conduct of business operations.
 27. Where the CMSA licensee is unable to complete CDD measures, it shall terminate the business relationship and consider if the circumstances are suspicious so as to warrant the filing of a suspicious transaction report (STR).
 28. A CMSA licensee shall perform such CDD measures as may be appropriate to its existing customers having regard to its own assessment of materiality and risk.
 29. In the case of a joint account, a CMSA licensee shall perform CDD measures on all of the joint account holders as if each of them were individually customers of the CMSA licensee.
 30. A CMSA licensee that undertakes any transaction with a non-account holder shall-
 - (a) establish and verify the identity of the customer as if the customer had applied to the CMSA licensee to establish business relations; and
 - (b) record adequate details of the transaction so as to permit the reconstruction of the transaction, including the nature and date of the transaction, the type and amount of currency involved, the value date, and the details of the payee or beneficiary.
 31. Where a CMSA licensee suspects that two or more transactions are or may be related, linked or the result of a deliberate restructuring of an otherwise single transaction into smaller transactions in order to evade the measures provided for in these Regulations, CMSA licensee shall treat the transactions as a single transaction and aggregate their values for the purpose of these Regulations.
 32. A CMSA licensee shall, in relation to politically exposed persons as defined in the Act, perform enhanced CDD measures in addition to normal CDD measures, including but not limited to the following-
 - (a) implement appropriate internal policies, procedures and risk management systems to determine if a customer or beneficial owner is a politically exposed person;
 - (b) obtain approval from the CMSA licensee's senior management to establish or continue business relations where the customer or beneficial owner is a politically exposed person or subsequently found to be or subsequently becomes a politically exposed person;
 - (c) take reasonable measures to establish the source of wealth and source of funds of the customer or beneficial owner; and
 - (d) conduct, during the course of business relations, enhanced monitoring of business relations with the customer.
 33. A CMSA licensee shall perform enhanced CDD measures in paragraph 32 for such other categories of customers, business relations or transactions as the CMSA

Anti-Money Laundering

G.N. No. 289 (contd.)

- licensee may assess to present a higher risk for money laundering and terrorist financing.
34. A CMSA licensee shall give particular attention to business relations and transactions with any person from or in countries and jurisdictions known to have inadequate AML/CFT measures, as determined by the CMSA licensee for itself or notified to CMSA licensees generally by the FIU.
 35. A CMSA licensee shall put in place policies and procedures to address any specific risks associated with the use of new technologies and non-face-to-face business relations or transactions.
 36. A CMSA licensee shall implement the policies and procedures referred to in paragraph 35 when establishing customer relationships and when conducting ongoing due diligence.
 37. Where there is no face-to-face contact, the CMSA licensee shall carry out CDD measures that are as stringent as those that would be required to be performed if there were face-to-face contact.
 38. A CMSA licensee may rely on an intermediary to perform CDD measures in accordance with the Act and these Regulations if the following requirements are met-
 - (a) the CMSA licensee is satisfied that the intermediary it intends to rely upon is subject to supervision for compliance with AML/CFT requirements consistent with standards set by the FATF, and has adequate measures in place to comply with those requirements;
 - (b) the intermediary is not one on which CMSA licensees have been specifically precluded by relevant Tanzanian authorities from relying; and
 - (c) the intermediary is able and willing to provide, without delay, upon the CMSA licensee's request, any document obtained by the intermediary which the CMSA licensee would be required or would want to obtain.
 39. No CMSA licensee shall rely on an intermediary to conduct ongoing monitoring of customers.
 40. Where a CMSA licensee relies on an intermediary to perform the CDD measures, it shall-
 - (a) document the basis for its satisfaction that the requirements in paragraph 38 have been met, and
 - (b) immediately obtain from the intermediary the information relating to CDD measures obtained by the intermediary.
 41. Notwithstanding the reliance upon an intermediary, the CMSA licensee shall remain responsible for its AML/CFT obligations as required under the Act, these Regulations and Guidelines.
 42. A CMSA licensee shall monitor on an ongoing basis, its business relations with customers.
 43. A CMSA licensee shall, during the course of business relations, observe the conduct of the customer's policy and scrutinize transactions undertaken to ensure that the transactions are consistent with the CMSA licensee's knowledge of the customer, its business and risk profile and where appropriate, the source of funds.
 44. A CMSA licensee shall pay special attention to all complex or unusually large transactions or unusual patterns of transactions that have no apparent or visible economic or lawful purpose.

Anti-Money Laundering

G.N. No. 289 (contd.)

45. A CMSA licensee shall take reasonable steps to inquire into the background and purpose of the transactions in paragraph 44 and document such information and its findings.
46. A CMSA licensee shall periodically review the adequacy of customer identification information obtained in respect of customers and beneficial owners and ensure that the information is kept up to date, particularly for higher risk categories of customers.

F. COLLECTIVE INVESTMENT SCHEMES (CIS)

1. No CIS manager shall deal with any person on an anonymous basis or any person using a fictitious name.
2. A CIS manager shall perform CDD measures when –
 - (a) unit holders subscribe or take part in the CIS;
 - (b) the CIS manager enters into negotiations with a entity with a view to signing a trust deed for establishment of a CIS;
 - (c) there is a suspicion of money laundering or terrorist financing; or
 - (d) the CIS manager has any doubt about the veracity or adequacy of information being provided.
3. A CIS manager shall establish the identity of each customer who signs an agreement to acquire or repurchase units or shares of a scheme.
4. For the purpose of the paragraph 3, a CIS manager shall obtain and record information of the customer, including but not limited to the following:
 - (a) in case of natural persons; full name, age, physical address, occupation, residence, and other particulars that will enable the identification of the individual;
 - (b) in case of legal persons-
 - (i) incorporation status, or in a case of a branch of a foreign company, place of incorporation or registration as may be appropriate;
 - (ii) the incorporation number or business registration number;
 - (iii) registered or business address and contact telephone number(s);
 - (iv) names and particulars of shareholders, if the immediate shareholder is a holding company to determine the ultimate or beneficial shareholders; and
 - (v) names, addresses and nationalities of directors.
5. The CIS manager shall verify the identity of a customer using reliable, independent sources.
6. The CIS manager shall retain copies of all reference documents used in identity verification and the identification information.
7. The CIS manager shall inquire if there exists any beneficial owner in relation to a customer. “Beneficial owner”, in relation to a customer of a CIS manager, means the natural person who makes final decisions, ultimately controls a customer or the person on whose behalf a transaction is being conducted and includes the person who exercises ultimate effective control over a body corporate or unincorporated.
8. Where there is one or more beneficial owners in relation to a customer, the CIS manager shall take reasonable measures to obtain information sufficient to identify

Anti-Money Laundering

G.N. No. 289 (contd.)

- and verify the identity of the beneficial owner(s).
9. Where the customer is not a natural person, the CIS manager shall take reasonable measures to understand the ownership and structure of the customer.
 10. The CIS manager shall not be required to inquire if there exists any beneficial owner in relation to a customer that is –
 - (a) a Tanzanian government entity;
 - (b) a foreign government entity, provided it is not sanctioned or blacklisted by the international community such as the United Nations or FATF;
 - (c) an entity listed on the stock exchange in Tanzania;
 - (d) an entity listed on a stock exchange outside of Tanzania that is subject to adequate regulatory disclosure requirements;
 - (e) a financial institution supervised by the Bank of Tanzania, CMSA or Tanzania Insurance Regulatory Authority;
 - (f) a financial institution incorporated or established outside Tanzania that is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF;
 - (g) a pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest under the scheme,unless the CMSA licensee suspects that the transaction is connected with money laundering or terrorist financing.
 11. For the purposes of items (d) and (f) of paragraph 10, a CIS manager shall document the basis for its determination that the requirements in those paragraphs have been duly met.
 12. Where a customer appoints one or more natural persons to act on his behalf in establishing business relations with the CIS manager or the customer is not a natural person, the CIS manager shall-
 - (a) identify the natural persons that act or are appointed to act on behalf of the customer, as if such persons were themselves customers;
 - (b) verify the identity of these persons using reliable, independent sources; and
 - (c) retain copies of all reference documents used to verify the identity of these persons.
 13. In the case of private trusts, the CIS manager shall verify the authorization given to each trustee of the relevant trust.
 14. The CIS manager shall verify the due authority of such person to act on behalf of the customer, by obtaining, including but not limited to, the following:
 - (a) the appropriate documentary evidence that the customer has appointed the persons to act on its behalf; and
 - (b) the specimen signatures of the persons appointed.
 15. Where the customer is a Tanzanian government entity, the CIS manager shall be required to obtain information as may be required to confirm that the customer is a Tanzanian government entity as indicated.
 16. Where a CIS Manager ("acquiring Manager") acquires, either in whole or in part, the business of another CIS Manager, the acquiring Manager, shall perform CDD

Anti-Money Laundering

G.N. No. 289 (contd.)

- measures on customers acquired with the business at the time of acquisition, except where the acquiring Manager has-
- (a) acquired at the same time all corresponding customer records (including information on natural persons appointed to act or are acting on behalf of the customer) and has no doubt or concerns about the veracity or adequacy of the information so acquired; and
 - (b) conducted due diligence enquiries that have not raised any doubt on the part of the acquiring Manager as to the adequacy of AML/CFT measures previously adopted in relation to the business or part thereof.
17. The Trustee of the acquired scheme shall ensure that the new manager fully complies with these Regulations.
 18. A CIS manager shall obtain, from a customer, when processing an application to establish business relations, information as to the purpose and intended nature of business relations.
 19. No CIS manager shall act as manager for a CIS unless the manager has completed CDD measures in relation to that customer.
 20. Where the CIS manager is, for any reason, unable to complete CDD measures on a customer, he shall not enter into a business relationship with that customer and shall instead consider if the circumstances are suspicious so as to warrant the filing of an STR.
 21. A CIS manager shall have at least one face-to-face contact with a customer before allowing that customer to hold units or shares in the CIS.
 22. Where there is no face-to-face contact, the CIS manager shall carry out CDD measures that are as stringent as those that would be required to be performed if there were face-to-face contact.
 23. A CIS manager shall observe conduct of the customer especially the customer's transactions to ensure that such transactions are generally consistent with the CIS Manager's knowledge of the customer.
 24. A CIS manager shall pay special attention to the transactions conducted by a customer that have no apparent or visible economic or lawful purpose.
 25. A CIS manager shall, to the extent possible, inquire into the background and purpose of the transactions and document their findings with a view to making this information available to the relevant competent authorities, should the need arise.
 26. A CIS manager shall periodically review the adequacy of customer identification information obtained in respect of customers and ensure that the information is kept up to date.

Dar es salaam,
27th August, 2012

WILLIAM AUGUSTAO MGIMWA,
Minister for Finance