Circular No (8/2014): Regulatory and Supervisory requirements for the Institutions under the Supervision of Central Bank of Sudan

Date: 9 September 2014
CBS/ BSRDD/ Circulars

Circulars of the Public Administration for Banking System Regulation and Development
Circular No (8/2014)

Addressed to all Institutions under the supervision of Central Bank of Sudan

Subject: Regulatory and Supervisory requirements for the Institutions under the Supervision of Central Bank of Sudan on Anti-money Laundering and Combating the Financing of Terrorism

In line with the efforts of the Central Bank of Sudan to develop regulatory and supervisory requirements on Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT), keeping up with global and local developments in this area, and based on the provisions of Article (44) of the "Anti-Money Laundering/Combating the Financing of Terrorism Law of 2014" and Article 8-2 of the "Banking Business Act of 2004", thereby, Circular No. 2/2014 on combating money laundering and terrorist financing shall be cancelled and be replaced with this circular.

I. Scope of the circular:

This circular shall apply to all institutions under the supervision of the Central Bank of Sudan (CBOS) as per the definition of an institution in paragraph (II) below. The institution shall ensure that it's local and foreign branches and majority-owned subsidiaries (50% and above) apply the AML/CFT regulations in this circular. If the requirements set out under Sudan's regulations are inconstant with those of the host country, the stricter of the two regulations shall be applied. In case of any impediments to applying these regulations to foreign branches or majority-owned subsidiaries, the CBOS shall be notified immediately.

II. Interpretation:

In this circular, unless the context requires otherwise, the following words and phrases shall have the following meanings wherever they appear:

Law shall mean the "Anti-Money Laundering /Combating the Financing of Terrorism Law of 2014".

Funds shall mean financial and non-financial assets and all types of properties, whether tangible or intangible, movable or immovable, regardless of how they were acquired, legal instruments and documents in any form, including electronic or digital, that prove a claim to

or benefit from such assets, including bank credits, traveler's checks, bank checks , payment orders, shares, securities, promissory notes, letters of credit, and any other interest, profit, or income derived from these funds or other assets.

Money Laundering shall mean the offenses criminalized under Article 35 of the law.

Financing of Terrorism shall mean the offenses criminalized under Article 36 of the law.

Unit shall mean the Financial Information Unit (FIU) established under Article (12) of the Law.

Person shall mean any natural person, legal person, or legal arrangement.

Institution shall mean any bank, foreign exchange company, money transfer company, leasing company, micro-financing institution (MFI), or any other financial institution licensed by the Central Bank of Sudan (CBOS) to provide specific financial activity.

Control shall mean the direct or indirect ability of a person to exercise significant influence on the decisions or actions of another person, including financial ones.
Control over the legal person or legal arrangement includes:

a. Possessing the ability, individually as a result of exercising voting rights, to appoint or remove the majority of members of the board of directors or supervisory body of the legal person or legal arrangement.

b. Possessing the ability to individually control the majority of members or shareholders of the legal arrangement or legal person under an agreement with the other members or shareholders of such legal arrangement or legal person.

c. Having the right to effectively control the legal person or legal arrangement under an agreement signed with the legal person or legal arrangement, or by virtue of an article of its Memorandum of Association or bylaws, if the law governing the legal person or legal arrangement permits so.

d. Having the authority to impose the effective control mentioned in paragraph (c) without such person having that right.

e. Having the right to use all properties of the legal person or legal arrangement or a part thereof,

f. Participating jointly or individually in bearing the financial responsibility of the legal person or legal arrangement or guaranteeing them.

g. Possessing the ability to control in any way, including the use of illegal means.

Beneficial owner shall mean the natural person who ultimately owns or exercises direct or indirect control over a customer, including the natural person on whose behalf a transaction is conducted and any natural person who exercises ultimate, actual control over a legal person or legal arrangement.

Business relationship shall mean a relationship which is established between an institution and its client and which is connected to the activities or services provided by the institution to the client, whenever the concerned institution expects the relationship to continue for a period of time.

Casual customer shall mean a customer that does not have a continuous business relationship with the institution.

Politically exposed persons (PEP) shall mean persons who are or have been entrusted with:

a. Prominent public functions domestically or in a foreign country, such as heads of state or governments, high-level politicians, high-level government officials, high-level judicial and military officials, senior executive officers in state-owned companies, and officials of key political parties.

b. Prominent functions by international organizations, who are members of the senior administration, i.e., directors, deputy directors, members of the board of directors, or equivalent posts.

Close associate shall include widely and publicly known close business colleagues and/or personal advisors of politically exposed persons, particularly financial advisors or persons acting in a financial legal capacity.

Family members shall include individuals related to politically exposed persons, directly (parents, brothers, sisters, sons and daughters) or through marriage.

Shell Bank shall mean a bank which has no physical presence in the state in which it is established and from which it obtained a license, and which is not subordinate to any financial group subject to regulation and effective consolidated banking supervision.

Private Banking shall mean activities through which the institution provides financial services to high net worth customers, usually via a central liaison officer between the institution and the client. Such officer facilitates the use of services and financial products offered by the institution to the customer.

Legal arrangement shall mean a relationship established pursuant to a contract between two or more parties that does not result in the emergence of a legal person, such as trusts.

Numbered Account shall mean an account opened with an institution where the customer is identified with a number instead of a name, and information about the customer is available only to a limited number of the institutions' employees.

Correspondent banking shall mean the provision of banking, payment and other services by an institution (the correspondent) to another institution (the respondent) to enable the latter to provide services and products to its own customers.

Non-profit organizations and association shall mean organizations and associations established under the "Law on the Organization of Humanitarian and Voluntary Work of 2006" or any other law that may replace it. It aims to provide social services and is not

intended to achieve any financial or personal gain. These include non-governmental organizations (NGOs), civil society organizations, and charities both domestic and foreign.

III. Money laundering (ML) and terrorist financing (TF) Risk assessment:

1. The institution must identify, assess and monitor the risks of ML/TF to which it may be exposed and must update the assessment bi-annually. The risk assessment must be appropriate to the nature and size of the institution. The institution shall document the risk assessment, its updates and all information related to these assessments, and has appropriate mechanisms in place to provide risk assessment information to competent authorities.

2. When identifying and assessing risks of ML/TF, and developing a system to manage and control these risks, the institution shall take into account the following categories of risk:

a. Customer risk factors.

b. Risks related to specific geographic areas.

c. Risks related to products and services.

d. Risks related to products and services delivery channels.

Customer risk factors:

Customer risk factors Include risks related to the identification of the customer or beneficial owner or their transactions or activities, examples include:

- Difficulties to identify the beneficial owner due to the complexity of the ownership structure of the legal persons.
- Non-resident customers.
- Legal persons issuing bearer shares.
- PEPs, their close associates and family members.
- Customers engaged in cash-intensive economic activities.
- Senior depositors and or customers whose source of wealth is unclear.
- Customers who do not deal face to face with the institution.
- Beneficial owners who control the legal person without control over its ownership.

Geographic risk factors:

Geographic risk factors Include risks related to the country of nationality of the customer, his place of residence or work, or the source or destination of his transactions, in terms of the adequacy of AML/CFT system in such country. Examples include:

- Countries that do not apply the recommendations of the Financial Action Task Force (FATF), or that do not apply them adequately.
    - Countries subject to sanctions, embargos or similar measures issued by the United Nations.
- Countries classified as offshore financial centers (OFC) or tax havens.
- Countries with a poor rating in terms of transparency.

- Countries classified as providing funding or support for terrorism, or suffering from drug or human trafficking.

Risks related to products and services:

Risks related to products and services Include risks associated with the characteristics of products and services, which can be exploited for money laundering or terrorism financing. Examples include:

- Cross-border wire transfers.
- Private Banking services.
- Stored-value cards.
- Services that do not allow the disclosure of most information concerning the identity of its users.
- Services that are identified by the CBOS as high risk services.

Risks related to services and products delivery channels:

Risks related to services and products delivery channels Include risks associated with the characteristics of the delivery of products and services, which are often associated with the use of modern techniques and technology that can be exploited for ML/TF due to simplified procedures for Customer Due Diligence (CDD), or to the fact that it allows the customer to transact remotely or execute a large number of transactions in a short period of time, as well as other advantages. Examples include:

- Financial services provided via mobile phone or online.
- Non face to face business relationships.

3. The institution shall take the following actions to manage and mitigate any identified risks:

a. Assess risk factors, including:

- The purpose behind opening an account or establishing a business relationship.
- The size of deposits or transactions conducted by the customer.
- The nature of the customer's economic activity and source of his funds.
- The frequency of transactions or duration of the business relationship.

b. Obtain additional information about the customer, the beneficial owner, the intended nature of the business relationship and the transaction.

c. Establish a risk profile on customers and transactions to include determining risk category (high - normal - low) for each customer. The profile must be updated periodically or whenever there are changes in the information available about the customer or their pattern of transactions. The customer profile should be based upon sufficient knowledge of thecustomer and beneficial owner as applicable, including the customer's anticipated business with the institution, and -where necessary- the source of funds and wealth of the customer.

d. The implementation of the enhanced due diligence procedures on high risk customers.

e. Taking into account all relevant risk factors before identifying the overall level of risk and the appropriate level of risk mitigation measures to be applied.

f. Updating all customer information on a regular basis.

g. Documenting risk assessment processes.

IV. Customer Due Diligence (CDD):

Customer Due Diligence (CDD)procedures:

4. CDD means carrying out a number of procedures including:

a. Customer identification and verification using original documents, data or reliable information from independent sources, and as described in this circular for each category.

b. Obtain and verify proof of the identity of any person acting on behalf of a customer, including evidence that such person is properly authorized to act in that capacity.

c. Identifying beneficial owners and taking reasonable steps to verify their identity.

d. Understanding the ownership and control structure of the legal persons or legal arrangements.

e. Understanding and obtain information on the purpose and intended nature of the business relationship.

f. Applying continuous CDD measures on business relationships using automated systems to monitor and identify customer pattern, and review any transactions conducted to ensure they are consistent with such patterns, the customer's commercial activities and risk profile, and – where necessary – the source of funds. Monitoring includes pre-set limits on the amount, size and type of transactions to be executed.

g. Updating the information, data and documents that were collected as part of CDD measures on an ongoing basis, especially for high-risk customers, and periodically checking their validity by reviewing existing records at an adequate frequency as determined by the institution.

5. The institution shall apply all CDD measures set out in this provision but may determine the extent of each measure using a risk based approach.

6. The institution shall carry out CDD measures itself, and shall not rely on any third party to carry out these procedures.

When to apply CDD:

7. Institutions shall apply CDD measures :

a. Before establishing a business relationship with a customer or before opening an account.

b. Before executing a transaction for a casual customer in an amount equal to or above the equivalent of 15,000 Euros in local or foreign currency, whether executed as a single transaction or as several transactions that appear to be linked.

c. Before executing local or international wire transfers.

d. Whenever the institution has doubts concerning the veracity or accuracy of the customer due diligence information previously obtained.

e. Whenever there is suspicion of ML/TF.

Timing of CDD measures:

8. A business relationship may be established or a transaction be carried out prior to verification of the customer or beneficial owner's identity provided that:

a. Postponing verification procedures is essential in order not to interrupt the normal conduct of business

b. The institution completes due diligence procedures as soon as possible.

c. The institution has taken the necessary measures for prudent management of the ML/FT risk for the case in which the delay was applied, including a limit on the number, type and value of transactions that can be executed before the completion of the verification procedures.

9. If the institution fails to meet the CDD measures mentioned in paragraph (4) above, it shall not open an account or establish any business relationship with the customer or perform any transaction to his account. It also must terminate the business relationship at the inability to meet the CDD measures for business relationships that existed before the entry into force of this circular, or if the institution cannot complete the CDD measures due to postponement as stated in paragraph (8) above. In all these cases, the institution must consider filing a Suspicious Transaction Report (STR) to the Unit.

10. In cases where the institution forms a suspicion of ML/TF, and it reasonably believes that carrying out CDD measures will tip-off the customer, it is permitted not to pursue the CDD process and instead file an STR to the Unit.

11. The institution shall also apply CDD measures to customers that existed before the entry into force of this circular on the basis of materiality and risk, and shall conduct CDD on such existing relationships at appropriate times, taking into account whether and when CDD measures have previously been undertaken and the adequacy of data obtained.

Identification and verification procedures:

12. Institutions shall use official identification documents to identify the customer, verify the documents' validity and keep a copy of these documents signed by the competent employee, stating that these are a replica of the official and valid document.

13. **Procedures to identify and verify the identity of a natural person:**

a. The institution shall verify the identity of the natural person using valid official documents (national identity card, driver's license, military card, judicial card, Police card, residency papers, passport or travel document), taking into account that the identification data includes full name of the customer , nationality, date of birth, address of permanent residence, phone numbers, work address, type of activity, purpose of the business relationship, names of delegates to deal with the account and their data, and any other information the organization deems necessary to obtain.

b. In case another person deals with the institution on behalf of the customer, the institution shall obtain a power of attorney allowing the person to do so, and keep an authenticated copy of it. The institution shall also identify and verify the identity of that other person in accordance with the procedures applicable to identifying the customer.

c. The institution shall take the necessary procedures to verify the validity of the data and information obtained from the customer, including by contacting competent authorities that issued the identity documents if there is doubt on the validity of these documents.

For other business relationships with natural persons, the institution shall verify their identity through documents identified in the circulars of the CBOS, and the information contained therein as follows:

Joint Accounts:

- Providing the necessary identification papers for each partner.
- Identifying account management responsibility, whether individually or jointly.

Accounts of trustees and executors of wills:

- Providing the necessary identification papers for each of the trustees and executors of wills.
- Providing a statement of appointment as a trustee provided it is issued by the competent court.
- Providing the trusteeship or wardship and adherence to the conditions stipulated in any of them.

Account of inheritance managers:

- Providing the legal “Decree of Distribution”.
- Providing the necessary identification papers for each of the inheritance managers.
- Providing the Sharia’a court decision or the Director General of Inheritance Affairs which has been designated as manager for the inheritance.

Employees' accounts:

- Providing a salary certificate from the employer.
- Providing the necessary identification papers for any employee.

14. **Procedures to identify and verify the identity of legal persons:**

a. Identification data of a legal person includes: the name of the legal person, the legal form, the headquarters address, type of activity, capital, the names of delegates to manage the account and their nationalities and phone numbers, the purpose of the business relationship, and any other information the institution deems necessary to obtain. The institution shall also verify the identity of the legal person and obtain an official proof of its existence (Certificate of incorporation or other official documents).

b. Obtaining a copy of documents proving the authorization from the legal person to a person representing them or the commissioning of natural persons to manage the account, in addition to the need to identify the authorized persons in accordance with the customer identification procedures stipulated in this Circular.

c. Obtaining the names and addresses of partners. For public companies, a list of the names and addresses of shareholders must be obtained.

For business relationships with legal persons, institutions must verify the existence of the legal person trough the appropriate documents and the information contained therein as follow:

Partnership accounts:

- Registration certificate of the business name issued from the Business Registrar or partnership registration certificate if registered under the name of one or more of the partners.

- Partnership Contract authenticated and sealed by the Administration of Courts pointing out the names and addresses of partners, and identifying the persons authorized to sign on the account either jointly or individually.

Corporate Accounts:

- Certificate of registration of the company issued by Business Registrar and a certificate of business commencement for public companies.

- Commercial license issued by the competent authority for companies and organizations registered in Sudan in addition to specimen signatures. For companies and institutions registered outside Sudan, documents issued by the foreign Registration Authority and authenticated in Sudan shall be provided.

- Article of Association and bylaws.

- The company's address and headquarters.

- The decision of the Board of Directors to open an account at the institution.

- The decision of the Board of Directors to appoint authorized persons to manage the company’s accounts and limits of their powers.

The accounts of government units and public corporations:

- The approval of the competent authority to which the government unit is affiliated or of the general manager of the establishment or corporation, as the case may be, to open the account.
- Approval of the Federal or State-level Ministry of Finance as the case may be.
- Mandate specifying the names of the persons authorized to sign on the account and the limits of their powers signed by the head of the government unit or the Director General, as the case may be.
- Copy of the law under which the government corporation or unit was established.

Accounts of Non-profit organizations and associations:

- Certificate of registration from the competent authority. For organizations and associations registered outside Sudan, documents issued by the foreign Registration Authority and authenticated in Sudan shall be provided.
- A copy of the Constitution and the Regulations which govern and regulate the work of such entities.
- The decision to establish the Executive Committee and appoint the three officers certified by the Corporations' Registrar.
- A letter specifying the bank in which the checking (current) account is to be opened signed by the head or secretary and mentioning the names of the persons authorized to sign on behalf of the relevant party and the limits of their powers to use that account.
- Identify and verify the identity of donors and beneficiaries of the deposited and withdrawn funds.

15. **Procedures to identify and verify the identity of legal arrangements:**

a. Identification data includes: the name of the legal arrangement, headquarters address, if any, the purpose of the legal arrangement, the name of the settlor, the trustee, beneficiaries and anyone else who exercises ultimate control over this legal arrangement, phone numbers, the purpose of the business relationship, and any other information the organization deems necessary to be obtained.

b. Obtaining a copy of documents proving the authorization from the legal arrangement to a person representing them or the commissioning of natural persons to manage the account, in addition to the need to identify the authorized persons in accordance with the customer identification procedures stipulated in this Circular.

Identification of the beneficial owner:

16. In order to make sure whether the customer is acting on behalf of one or more beneficial owner, the institution shall request each customer when opening an account to sign an affidavit which discloses information about the beneficial owner of the business relationship to identify him. The institution can take other measures to determine the identity of the beneficial owner through any other sources as it deems necessary.

17. The institution shall identify the beneficial owners and take reasonable steps to verify their identity using reliable, independent source documents, data or information, such that the institution is satisfied it knows who the beneficial owner is. For legal persons and legal arrangements, this should include the understanding by the institution of the ownership and control structure of the customer.

18. The identification of the beneficial owner for legal persons and legal arrangements is carried out as indicated below:

a. For legal persons, the institution must identify each natural person who owns or controls, directly or indirectly, more than 10% of the legal person. If the institution fails to confirm that this person is actually the beneficial owner or finds that no natural person is exercising control through ownership, then the identity of each natural person who exercises control by other means shall be specified. In case this abovementioned specification is not possible, the institution must determine the identity of the person responsible for the management of the legal person.

For customers listed in the Khartoum Stock Exchange (KSE), the institution is not required to identify the shareholders or beneficial owners or to verify their identity. This procedure does not absolve the institution from obtaining copies of the documents required to verify the identity of the legal person as stated in paragraph (14) above.

b. For legal arrangements, the institution must verify the identity of the settlor, the trustee and the Secretary (if any), all beneficiaries, and any other natural person who ultimately exercises direct or indirect effective control over the legal arrangement.

Enhanced due diligence:

19. Institutions should examine, as far as reasonably possible, the background and purpose of all complex, unusual transactions, and all unusual patterns of transactions which have no apparent economic or lawful purpose. Where the risks of money laundering or terrorism financing are higher, institutions shall conduct enhanced due diligence, consistent with the risks identified. Institutions shall increase the degree and nature of monitoring of such business relationships, and determine whether those transactions or activities are suspicious. Institutions need to keep records for these

transactions regardless of the decision taken, and make records available to the competent authorities and auditors upon request.

20. In addition to the regular CDD measures, the institution shall apply Enhanced CDD measures for high-risk business relationships. Examples of these procedures include:

a. Obtaining additional documents and information related to the customer and the beneficial owner, contact information and residence.

b. Obtaining additional documents and information related to specifying the profession, source of funds, the source and nature of wealth, business relationships with other institutions, the intended nature of the business relationship, and the purpose of intended or performed transactions.

c. Updating documents, information and data on customers and beneficial owners more frequently, and conducting a periodic review of the business relationship and enhanced monitoring of transactions.

d. Obtaining the approval of the senior management to establish/continue the business relationship.

21. The institution must apply enhanced due diligence procedures, according to identified risks, on business relationships and transactions with persons bearing the nationality of or residing in countries that do not apply the recommendations of the FATF or that do not apply them adequately. In high risk cases, the institution shall limit its transactions with such customers and consider the termination of the business relationship.

22. The institution must include in its policies efficient procedures for business relationships conducted without the customer being physically present, so that it is strict in the customer identification and verification process. Examples of these procedures include:

a. Requesting certification of documents presented by the customer when establishing a business relationship.

b. Requesting additional documents to verify their identity or contact information, wealth, source of funds, and other elements.

c. Obtaining the recommendation of an independent third party to identify the customer.

d. Putting restrictions on transactions of the account such as limiting the amount and type of transactions that can be executed.

e. Conducting ongoing enhanced monitoring of the business relationship to check if transactions appear to be unusual or suspicious.

V. Other controls to establish business relationships:

23. The institution is not allowed to open, retain, or deal with any numbered accounts.

24. The institution is not allowed to open or retain anonymous accounts or accounts under fictitious names.

25. Before establishing a business relationship with a customer, the institution shall verify that the customer's name is not included in lists of defaulters or blacklisted customers issued by the CBOS. It shall not perform any transaction for a blacklisted casual customer. If the institution discovers that it had existing business relationships with blacklisted/defaulting customers before the entry into force of this circular, it should immediately file a Suspicious Transaction Report to the Unit.

26. Approval must be obtained from the branch manager or anyone acting on his/her behalf to enter into a business relationship with any customer.

27. No employee in any institution shall manage any account on behalf of a customer.

VI. Cases requiring special measures:

In addition to CDD measures stipulated in paragraph IV of this circular, the institution shall take special measures in the following cases:

Politically exposed persons

28. The institution shall develop an appropriate risk management system that determines whether a customer or beneficial owner is a PEP. This system shall include the following as a minimum:

a. Requesting a declaration from the customer and beneficial owner including relevant information.

b. Verifying the available information about the customer and beneficial owner.

c. Searching in commercial electronic databases for PEPs, if available.

29. If the institution establishes that a customer or beneficial owner is a PEP, it shall do the following:

a. If the PEP is a person that is or has been entrusted with a prominent public function in a foreign country:

- obtain approval from senior management before establishing or continuing a business relationship with such person;
- take reasonable measures to identify the source of wealth and source of funds;
- apply enhanced ongoing monitoring to the business relationship to know whether the transactions appear unusual or suspicious.

b. If the PEP is a person who is or has been entrusted with a prominent function in Sudan or by an international organization and considered as a high risk customer, the measures referred to under (a) above shall be applied.

30. The institution shall apply these special measures also to family members and close associates of such PEPs.

Correspondent banking

31. In addition to performing basic customer due diligence pursuant to Chapter IV, the institution shall take the following measures when establishing a business relationship with a respondent institution:

a) Gather sufficient information about the respondent institution to understand fully the nature of its business and evaluate, using publicly available information or information provided upon request, the reputation of the respondent institution and the level of supervision to which it is subject, including whether the respondent institution or any of its board members or owners of its controlling stake has been subject to a money laundering or terrorist financing investigation or regulatory action.

b) Evaluate the anti-money laundering and combating the financing of terrorism controls implemented by the respondent institution and verify their efficiency and adequacy.

c) Obtain approval from senior management before establishing a new correspondent relationship.

d) Clearly understand and document the AML/CFT responsibilities of each institution with regard to correspondent services.

e) If payable-through accounts services are provided, the correspondent institution should be satisfied that the respondent institution has performed CDD obligations on its customers having direct access to such accounts and is able to provide relevant CDD information about these customers when necessary.

f) Institutions must not enter into or continue a business relationship with a respondent institution that is a shell bank or that allows its accounts to be used by a shell bank.

g) File a written questionnaire showing the position of the respondent institution regarding compliance with local AML/CFT legislation and supervisory controls, standards of due diligence applied by the respondent institution to its customers, and the availability of effective AML/CFT internal policies and procedures at the respondent institution.

32. The above measures should be applied to cross-border correspondent banking procedures and similar relationships that have been created before the entry into force of this circular.

Wire transfers:

33. Scope of execution:

a. The provisions of this paragraph shall apply to domestic and cross-border wire transfers in any currency.

b. These measures do not apply to transfers resulting from transactions using payment cards, discount cards, or any other similar payment method. All these types of transactions must be given a unique reference number to track the transaction back to the originator and beneficiary.

c. These measures do not apply to transfers or settlements made between financial institutions where both parties of the transfer are financial institutions working each for its own interest.

Obligations of originating institutions:

34. The institution originating the transfer shall obtain: A- full information about the transfer originator, including: a- the name, b- the account number, and c- the address or national identity number, or customer identification number of date and place of birth, and B- complete information about the beneficiary, including: a- the name, and b- the account number used to process the transaction. In the absence of an account number for the originator or the beneficiary, the institution shall give a unique transaction reference number to the transaction.

35. The originating institution shall verify the accuracy of the information about the originator before sending the transfer, using official documents and information, and include in the transfer form all the data referred to in paragraph (34) above.

36. Where several transfers from a single originator are bundled in a batch file for transmission to beneficiaries, the batch must contain all of the information mentioned in paragraph (34) above, to permit traceability of the transaction in the hosting country. The originating institution shall include the originator's account number or unique transaction reference number in the absence of an account number, provided that:

a. The institution has the ability to provide the beneficiary institution or competent authorities with all required information within three business days from the date of receipt of the request for information.

b. The institution responds immediately to any order issued by a competent law enforcement authority to access all required information.

c. Institution must be sure that no unusual transfers are sent in one bundle in situations that increase the risk of ML/TF.

37. The institution shall keep all data referred to in paragraph (34) above and the information and documents related hereto.

38. The institution shall not execute any wire transfer that does not comply with the requirements stipulated in paragraphs (34-37) above.

Obligations of beneficiary institution:

39. The beneficiary institution shall take reasonable measures, which may include post-execution monitoring or real-time monitoring, where feasible, to detect any wire transfers that lack the required originator or beneficiary information under paragraph (34) above.

40. If the identity of the beneficiary was not verified by the ordering institution when executing the transfer, the beneficiary institution shall identify and verify the customer's identity and maintain information and documents in accordance with record keeping measures in Paragraph VII of this circular.

41. The beneficiary institution shall adopt efficient risk-based policies and procedures to deal with transfers that lack required information contained in paragraph (34) above and to determine when to execute, reject or suspect a wire transfer lacking such information. These procedures may include requesting missing information from originating financial institution. In case of failure to obtain the required information, the institution must take risk-based action, possibly including the rejection of the transfer, filing a suspicious transaction report, or determining appropriate follow-up measures.

Obligations of intermediary institutions:

42. Any intermediary institutions involved in executing a wire transfer without being its originators or beneficiaries should ensure that all data required in paragraph (34) above and annexed to the wire transfer is retained with it.

43. Where technical limitations prevent the required information from remaining with the wire transfer, the intermediary institution shall keep a record, for at least five years, of all annexed information, regardless of completeness or lack thereof, and it should be able to provide this information to beneficiary financial institutions within one business day from the date of request.

44. Intermediary institutions should take reasonable measures to identify wire transfers that lack required originator and beneficiary information and adopt risk-based policies and procedures for determining:

a. When to execute, reject, or suspend a wire transfer lacking required data; and

b. The appropriate follow-up action.

Other obligations:

45. Any institution engaged in fund transfer activities should keep an updated list of its agents, and make it available to inspection teams upon request.

46. The institution shall immediately terminate any relationships with any respondent institution that does not adhere to the provisions of this circular regarding wire transfers.

New technologies:

47. Institutions shall identify, assess, and take appropriate measures to manage and mitigate the risks of ML/TF that may arise as a result of the following:

a) the development of new products and new business practices including new delivery mechanisms for services;

b) The use of new or developing technologies for both new and pre-existing products.

When providing payment services through mobile phone, institution shall, for example:

a. Ensure that they obtain information on transfers stipulated in this circular when using this service in the transfer of money.

b. Ensure the ability to stop the service in the event of misuse, and include this condition in the service contract.

c. Exercise ongoing monitoring of transactions and retrieval of unusual transaction reports generated by the use of such service.

d. Set reasonable limits to deposit into accounts used in this service, as well as the value of the transaction that can be executed.

VII. Book and record keeping

48. Institutions must keep records and data, supporting evidence to the business relationships, banking operations and due diligence procedures, and the results of screening of unusual transactions, including originals or copies of identity documents that would be acceptable to courts in accordance with the legislation in Sudan. Such records must be sufficiently detailed to permit the reconstruction of each individual transaction (including the amounts and types of currencies used if any). Such records and information shall be provided to competent authorities in a timely manner. Records and data include the following:

a. All records obtained through CDD measures, including documents proving the identity of customers and beneficial owners, accounting files and business correspondence, for at least five years following the termination of the business relationship or the date of a transaction carried out by a casual customer, whichever is longer.

b. Records and data of transactions, both local and international, executed or attempted, for a period of at least five years from the date of the transaction or attempted transaction. These records shall be detailed in a way that permits the reconstruction of each individual transaction.

c. Records and information relating to STRs submitted to the unit and related documents for at least five years after the date of notifying the Unit, and records relating to criminal lawsuits until they are resolved, even if the legally set record keeping period is exceeded.

d. Records relating to risk assessments and any relevant information for five years from the date of the assessment or its update.

e. Documented records of all AML/CFT training programs that took place during a period of not less than five years back. These records shall include the names of the trainees and their qualifications and training institution both at home and abroad.

VIII. Reporting suspicion transactions:

49. The compliance officer at the institution is the person in charge of reporting suspicious transactions to the Unit pursuant to Article 6 of the AML/CFT Law, using the reporting template designed by the unit for this purpose.

50. The institution must report to the unit immediately whenever it suspects or has reasonable grounds to suspect that any funds constitute proceeds or transactions or attempted transactions are linked to money laundering or terrorism financing.

51. If any employee suspects there is a relationship between the transaction and proceeds of crime or ML/TF, he/she should inform the compliance officer and attach all the data and copies of documents related to that transaction.

52. The compliance officer shall provide the data to the Unit, and facilitate its access to records and information in order to carry out its functions.

53. Institutions, their directors and employees are prohibited from disclosing to any person, directly or indirectly, by any means, the fact that a suspicious transaction report or any related information is being or has been submitted to the Unit or that a money laundering or terrorism financing investigation is being carried out. This does not preclude disclosures or communications between and among directors and employees of the institution, and with lawyers, competent authorities, and the public prosecution in that regard.

54. Any institution and its directors or employees who in good faith report or provide information about a suspicious transaction to the unit shall not be subject to any civil, criminal, or administrative liability for violation of any prohibition on the disclosure of information required by a contract or law.

IX. Internal control system:

55. Institutions shall develop an internal AML/CFT system that is appropriate having regard to the institutions' risk of money laundering and terrorism financing and the size of the business. The system shall include policies, procedures, internal controls, compliance, recruitment, training, and internal and external audit functions. Financial groups shall develop and implement policies and procedures to combat ML/TF at a group level, which should include mechanisms for exchanging information within the group and for maintaining confidentiality of the information exchanged.

The AML/CFT system shall include, as a minimum, the following:

a. Clear policy, procedures and internal controls to combat money laundering and terrorism financing, approved by the Board of Directors or Regional Director for branches of foreign institutions that are constantly updated, and that address the following as a minimum:

- A risk assessment at the institutional level and identifying a risk management system.
- Customer risk assessment, classification and identification of a risk profile.
- Customer acceptance and termination of the business relationship.
- Due diligence procedures and controls over delayed or enhanced CDD.
- Monitoring of operations and business relations.
- PEPs, correspondent banking relationships and wire transfers.
- Book and record keeping and updating.
- Suspicious transactions reports and non-disclosure of reporting.
- Compliance officer job description.
- Review mechanism and administrative controls.
- Standards of integrity and experience in the recruitment of staff.
- Continuous AML/CFT training programs for staff.
- The implementation of policies, procedures, controls and monitoring at the level of branches, subsidiaries and groups.
- Responding to requests from supervisory and other competent authorities and the Unit.

b. Appointment of a compliance officer and his deputy at the senior management level and working under the supervision of the Board of Directors, provided that they have appropriate academic qualifications and practical experience. The institution should inform the CBOS in the case of replacing either of them, and he/she shall have the following powers and responsibilities:

- Access to records and data as required for carrying out the work of the examination and review of systems and procedures established by the institution to combat ML/TF.
- To exercise his powers independently and be accountable to the Board of Directors in order to verify the extent of the implementation of the AML/CFT system in the organization.
- Receive information and reports on unusual or suspicious transactions to review and take the appropriate decision whether to notify the Unit or not, provided that the decision not to notify the Unit should be justified.

c. Developing plans and ongoing AML/CFT training programs for employees, board members, members of the executive management, supervisors and managers in co-operation with the compliance officer. These programs shall include AML/CFT techniques and how to detect and report offences and the developments in the area of risk assessment, mitigation and how to deal with suspicious customers.

d. Internal audit shall examine internal control systems to ensure their efficiency, and verify the staff's and compliance manager's execution of their responsibilities, and the extent of the staff's compliance to policies and procedures to combat ML/TF and include all results in his report to the management.

e. A mechanism for external auditing, to ensure implementation of this circular, the adequacy of policies and procedures related thereto, and the inclusion of the results of that in his report to the management.

f. The existence of accurate procedures for examination and investigation to ensure the existence of a high fit and proper test measures in the selection of applicants when recruiting new employees. These measures shall include accessing candidates' criminal records and considering any other information useful to confirm the absence of a conflict of interest or dishonesty or fraud.

X. Final provisions:

56. The external auditor of the institution shall notify the CBOS immediately upon discovery of any violation of this circular.

57. Institutions shall implement freezing orders, or refrain from carrying out transactions for persons specified by the authority designated to implement the resolutions of the Security Council of the United Nations pursuant to Chapter 7, on terrorism and the financing of terrorism and the financing of the proliferation of weapons of mass destruction, according to the provisions of Article 34 of the law.

58. Any person who violates this circular is subject to financial and administrative sanctions by law, and to penalties prescribed under the provisions of Articles 38 and 41 of the law.

This Circular shall come into force as of this date,

On behalf of Central Bank of Sudan

Elharam Ahmed Mohamed Mokhtar
Dr. Nagwa Sheikh Eldin Mohamed

Financial institutions directorate
Public Administration for Banking System Regulation and Development