BANK OF SOUTH SUDAN (BSS)
DIRECTORATE OF SUPERVISION, RESEARCH & STATISTICS
PLOT NO. 1, BLOCK 6, P.O.BOX 136, JUBA MARKET, JUBA

Circular No. DSR/SD/1/2017

To: All Financial Institutions Operating in the Republic of South Sudan

Subject: Customer due Diligence and guidelines on Know Your Customer (KYC) for Banks

This Circular is issued under the authority of Section 12 of the Bank of South Sudan Act 2011 (BSS Act), Section 77 of the Banking Act 2012 (Banking Act), and Section 16 of the Anti-Money Laundering and Counter Terrorism Financing Act, 2012 (AML-CTF Act). And prescribes the minimum standards for registering the identity of a person, natural or legal entity, who opens an account in the bank or otherwise uses the bank for financial activities. This Circular sets the minimum requirements that banks operating in South Sudan must implement and comply with. The Bank of South Sudan (BSS) encourages the banks to further develop and enhance their internal due diligence requirements in order to implement sound risk management practices and conduct their business activities in the most prudent manner.

This Circular shall be cited "as *Customer Due Diligence and Know Your Customer (KYC) for Banks, Circular no. DSR/SD/1/2017*, and shall come into effect as from the date of its signature by the Governor of the Bank of South Sudan.

I. Background

1. Consistent with ensuring that banks operating in South Sudan implement sound risk management practices and conduct their business activities in a prudent manner as required by Section 59(1) of the Banking Act, the Bank of South Sudan directs all banks to incorporate the principals and recommendations outlined in this Circular into their risk management policies. This Circular is based on principles outlined by the Basel Committee on Banking Supervision in its paper "*Customer due diligence for banks*" issued in October 2001, by Bank for International Settlements.

2. The principles outlined in this circular will assist banks in ensuring ongoing compliance with the requirements of Sections 77 and 78 of the Banking Act 2012. In addition, the adoption of these principles by banks licensed to operate in South Sudan will reduce the likelihood of domestic banks being

used for channelling proceeds of corruption, laundering funds obtained through criminal activities, or financing of terrorism.

3. Internationally supervisors are increasingly recognising the importance of ensuring that banks have adequate controls and procedures in place so that they know the customers with whom they are dealing. Adequate due diligence on new and existing customers is a key part of these controls. Without this due diligence, banks can become subject to reputational, operational, legal and concentration risks, which can result in significant financial cost.

4. Know Your Customer requirements (KYC) are most closely associated with the fight against money-laundering. The BSS' approach to KYC is from a wider prudential, not just anti-money laundering or financing of terrorism, perspective. Sound KYC procedures must be seen as a critical element in the effective management of banking risks. KYC safeguards go beyond simple account opening and record-keeping and require banks to formulate a customer acceptance policy and a tiered customer identification programme that involves more extensive due diligence for higher risk.

II. Essential elements of KYC standards

5. All banks are required to have in place adequate policies, practices and procedures that promote high ethical and professional standards and prevent the bank from being used, intentionally or unintentionally, by unidentifiable elements. Certain key elements should be included by banks in the design of KYC programmes. Such essential elements should start from the banks' risk management and control procedures and should include:

   a. customer acceptance policy;

   b. customer identification;

   c. ongoing monitoring of high risk accounts; and

   d. risk management.

   Banks should not only establish the identity of their customers, but should also monitor account activity to determine those transactions that do not conform with the normal or expected transactions for that customer or type of account. KYC should be a core feature of banks' risk management and control procedures, and be complemented by regular compliance reviews and internal audit.

III. Customer acceptance policy

6. Banks should develop clear customer acceptance policies and procedures, including a description of the types of customer that are likely to pose a higher than average risk to a bank. In preparing such policies, factors such as customers' background, country of origin, public or high profile position, linked accounts, business activities or other risk indicators should be considered. Banks should develop graduated customer acceptance policies and procedures that require more extensive due diligence for higher risk customers.

IV. Customer identification

7. Customer identification is an essential element of KYC standards. For the purposes of this Circular, the term "customer" shall mean:

   a. The person or entity that maintains an account with the bank or those on whose behalf an account is maintained (i.e. beneficial owners);

   b. The beneficiaries of transactions conducted by professional intermediaries; and

   c. Any person or entity connected with a financial transaction who can pose a significant reputational or other risk to the bank.

8. Banks should establish a systematic procedure for identifying new customers and should not establish a banking relationship until the identity of a new customer is satisfactorily verified.

9. Bank must take reasonable measures to satisfy themselves as to the true identity of the customer.

10. For one-off or occasional transactions where the amount of the transaction or series of linked transactions does not exceed USD 10,000 or equivalent in SSP or in any other currencies, it may be sufficient to require and record only name, address and official personal identification number stated in an unexpired official document.

11. Banks should document and enforce policies for identification of customers and those acting on their behalf. The best documents for verifying the identity of customers are those most difficult to obtain illicitly or to counterfeit. Special attention should be exercised in the case of non-resident customers and in no case should a bank short-circuit identity procedures just because the new customer is unable to present for interview. A bank should always ask itself why the customer has chosen to open an account in South Sudan.

12. The customer identification process applies naturally at the outset of the relationship. To ensure that records remain up-to-date and relevant, banks should undertake regular reviews of existing records. An appropriate time to do so is when a transaction of significance takes place, when customer documentation standards change substantially, or when there is a material change in the way that the account is operated. However, if a bank becomes aware at any time that it lacks sufficient information about an existing customer, it should take steps to ensure that all relevant information is obtained as quickly as possible.

13. Banks should develop clear standards on what records must be kept on customer identification and individual transactions and their retention period. These standards must meet at least the requirements stipulated in section 77 of the Banking Act, 2012. Such a practice is essential to permit a bank to monitor its relationship with the customer, to understand the customer's ongoing business and, if necessary, to provide evidence in the event of

disputes, legal action, or a financial investigation that could lead to criminal prosecution.

14. Banks should subject transactions with customers in jurisdictions that do not have adequate systems in place to prevent or deter money laundering or financing of terrorism to additional scrutiny to examine the background and purpose of the transaction.

V. General Identification Requirements

15. Banks should obtain all information necessary to establish their full satisfaction the true identity of each new customer and the purpose and intended nature of the business relationship. The extent and nature of the information depends on the type of applicant (personal, corporate, etc.) and the expected size of the account.

16. When an account has been opened, but problems of verification arise in the banking relationship that cannot be resolved, the bank should close the account and return the monies to the source from which they were received. The bank should immediately inform the BSS of any such event and provide any documentary evidence supporting its decision.

17. Banks should include originator information and related messages on funds transfers that should remain with the transfer throughout the payment chain. Originator information should include name, address, and account number (when being transferred from an account). Banks should give enhanced scrutiny to inward funds transfers that do not contain originator information. Should problems of verification arise that cannot be resolved, the bank should return the monies to the source from which they were received. The bank should immediately inform the BSS of any such event and provide any documentary evidence supporting its decision.

18. While the transfer of an opening balance from an account in the customer's name in another bank subject to the same KYC standard may provide some comfort, banks should nevertheless consider the possibility that the previous account manager may have asked for the account to be removed because of a concern about dubious activities. Naturally, customers have the right to move their business from one bank to another. However, if a bank has any reason to believe that an applicant is being refused banking facilities by another bank, it should apply enhanced diligence procedures to the customer. The bank should immediately inform the BSS of any such event and provide any documentary evidence supporting its decision.

19. Banks must not open an account or conduct ongoing business with a customer who insists on anonymity or who gives a fictitious name. It is an offence under Section 77 of the Banking Act to open or operate an account in a false name that may result in the BSS taking measures set forth in Section 115 of the Banking Act.

20. Banks must not open an account or conduct ongoing business with a customer without having conducted an in person interview with the customer

(natural persons) or one or more of its authorised representatives (legal persons).

VI. Specific Identification Issues

21. There are a number of more detailed concerns relating to customer identification, which is outlined below. The BSS will monitor international developments and issue further circulars and/or guidelines on the matter when required.

Personal customers

22. For personal customers (natural persons), banks must obtain the following information:

    a. Legal name and any other names used (such as maiden name);

    b. Correct permanent address (the full address should be obtained; a Post Office box number is not sufficient);

    c. Telephone number, fax number, and e-mail address;

    d. Date and place of birth;

    e. Nationality;

    f. Occupation, public position held and/or names of the past three employer, when applicable;

    g. An official personal identification number or other unique identifier contained in an unexpired official document (e.g. passport, identification card, residence permit, social security records, driving licence) that bears a photograph of the customer;

    h. Type of account and nature of the banking relationship; and

    i. Signature.

23. Banks must verify the information provided by all of the following methods, if applicable:

    a. Confirming the date of birth from an original official document (e.g. birth certificate, passport, identity card, driving license, social security records);

    b. Confirming the permanent address (e.g. an original utility bill, tax assessment, bank statement, a letter from a public authority);

    c. Contacting the customer by telephone, by letter or by e-mail to confirm the information supplied after an account has been opened (e.g. a disconnected phone, returned mail, or incorrect e-mail address should warrant further investigation);

    d. Confirming the validity of the official documentation provided through certification by an authorised person (e.g. local government official, notary public);

e. Seeking personal reference by an existing customer of the bank;

f. Requesting prior bank reference and contact with the bank regarding the customer;

g. Verifying source of income or wealth (e.g. an original payslip, letter from the employer);

h. Confirmation of employment or public position held (e.g. an original letter of employment or appointment);

i. The specimen signature must be provided in the presence of the bank's officer and kept in the account/customer file; and

j. Additional information related to nationality or country of origin, public or high profile position, etc.

Banks should verify all the above listed information against original identity and other documents issued by an official authority, make copies for the file, and have them signed by the bank's officer. Any subsequent changes to the above information should also be recorded and verified in a similar manner.

Corporate and other business customers

24. For corporate and other business customers, banks should obtain evidence of their legal status, such as an incorporation document, partnership agreement, association documents or a business licence. For large corporate accounts, a financial statement of the business or a description of the customer's principal line of business should also be obtained. In addition, if significant changes to the company structure or ownership occur subsequently, further checks should be made. In all cases, banks need to verify that the corporation or business entity exists and engages in its stated business. The original documents or certified copies of certificates should be produced for verification.

For corporate and other business customers, banks must obtain the following information:

a. Name of institution;

b. Principal place of institution's business operations;

c. Mailing address of institution;

d. Contact telephone and fax numbers;

e. Taxpayer Identification Number;

f. The original or certified copy of the Certificate of Incorporation and Memorandum and Articles of Association;

g. The resolution of the Board of Directors to open an account, if applicable, and identification of those who have authority to operate the account;

h. Signature(s); and

i. Nature and purpose of business and its legitimacy.

25. Banks should verify the information provided by all of the following methods:

a. For established corporate entities - reviewing a copy of the latest report and accounts (audited, if available);

b. Conducting an enquiry by a business information service, or an undertaking from a reputable firm of lawyers or accountants confirming the documents submitted;

c. Utilising an independent information verification process, such as by accessing public and private databases, if available;

d. Obtaining prior bank references, if applicable;

e. Visiting the corporate entity, where practical;

f. The specimen signature(s) must be provided in the presence of the bank's officer and kept in the account/customer file; and

g. Contacting the corporate entity by telephone, mail or e-mail.

26. For corporations/partnerships, the principal guidance is to look behind the institution to identify those who have control over the business and the company's/partnership's assets, including those who have ultimate control. For corporations, particular attention should be paid to shareholders, signatories, or others who inject a significant proportion of the capital or financial support or otherwise exercise control. Where the owner is another corporate entity or trust, the objective is to undertake reasonable measures to look behind that company or entity and to verify the identity of the principals. For partnerships, each partner should be identified and it is also important to identify immediate family members that have ownership control.

Politically exposed persons

27. Business relationships with individuals holding important public positions and with persons or companies clearly related to them may expose a bank to significant reputational and/or legal risks. Such politically exposed persons ("PEPs") are individuals who are or have been entrusted with prominent public functions, including heads of state or of government, senior politicians, senior government, judicial or military officials, senior executives of publicly owned corporations and important political party officials.

28. Accepting and managing funds from corrupt PEPs will severely damage the bank's own reputation, can undermine public confidence in the ethical standards of South Sudan's financial system, and may attract regulatory and/or criminal penalties. In addition, a bank may be subject to costly information requests and seizure orders from law enforcement or judicial authorities and could be liable to actions for damages by the state concerned or the victims of a regime. Under certain circumstances, a bank and/or its officers and employees themselves can be exposed to charges of money laundering, if they know or should have known that the funds stemmed from corruption or other serious crimes. In this regard, Section 78 of the Banking

Act imposes requirements on banks and their officers to satisfy themselves as to the bona fide nature of each transaction and to report any suspicious transactions to the appropriate authorities.

29. Banks should gather sufficient information from a new customer, and check publicly available information, in order to establish whether or not the customer is PEP. Banks should investigate the source of funds before accepting PEP. The decision to open an account for PEP should be taken at a senior management level.

VII. Retention of records

30. Customer identification documents, original or certified copies, should be retained for at least five years after an account is closed.

31. All financial transaction records should be retained for at least five years after the transaction has taken place.

VIII. Confidentiality of Information

32. No person who has acquired knowledge in his capacity as officer, employee or agent of the bank shall disclose to any person or governmental authority the identity, assets, liabilities, transactions or other information in respect of an account holder except -

    a. with the written authorisation of the account holder or of his heirs or legal personal representatives; or

    b. for the purpose of the performance of his duties within the scope of his employment in conformity with the provision of this Circular or other Regulations issued by the Bank of South Sudan; or

    c. when lawfully required to make disclosure by any court of competent jurisdiction within or outside South Sudan; or

    d. Under the provisions of any laws of South Sudan.

33. A bank whose officer, employee or agent is found to have contravened the provisions of Section 31 shall be liable to a fine not exceeding USD 50,000 or equivalent in SSP.

IX. Ongoing Monitoring of Accounts and Transactions

34. Ongoing monitoring is an essential aspect of effective KYC procedures. Banks can only effectively control and reduce their risk if they have an understanding of normal and reasonable account activity of their customers so that they have a means of identifying transactions which fall outside the regular pattern of an account's activity. Without such knowledge, banks are likely to fail in their duty to report suspicious transactions to the relevant authorities. The extent of the monitoring needs to be risk-sensitive. For all accounts, banks should have systems in place to detect unusual or suspicious patterns of activity. This can be done by establishing limits for a particular class or category of accounts. Particular attention should be paid to transactions that exceed these limits. Certain types of transactions should alert banks to the possibility that the customer is conducting unusual or

suspicious activities. They may include transactions that do not appear to make economic or commercial sense, or that involve large amounts of cash deposits that are not consistent with the normal and expected transactions of the customer. Very high account turnover, inconsistent with the size of the balance, may indicate that funds are being "washed" through the account.

35. There should be intensified monitoring for higher risk accounts. Every bank should set key indicators for such accounts, taking note of the background of the customer, such as the country of origin and source of funds, the type of transactions involved, and other risk factors. For higher risk accounts:

    a. Banks should ensure that they have adequate management information systems to provide managers and compliance officers with timely information needed to identify, analyse and effectively monitor higher risk customer accounts. For example, the types of reports could include reports of missing account opening documentation, transactions made through a customer account that are unusual, and aggregations of a customer's total relationship with the bank.

    b. Senior management in charge of banking business should know the personal circumstances of the bank's high-risk customers and be alert to sources of third party information. A senior manager should approve significant transactions by these customers.

    c. Banks should develop a clear policy and internal guidelines, procedures and controls, and remain especially vigilant regarding business relationships with PEPs and high profile individuals or with persons and companies that are clearly related to or associated with them. As all PEPs may not be identified initially and since existing customers may subsequently acquire PEP status, regular reviews of at least the more important customers should be undertaken, at a minimum every six months.

X. Risk Management

36. Effective KYC procedures embrace routines for proper management oversight, systems and controls, segregation of duties, training and other related policies. The board of directors of the bank should be fully committed to an effective KYC programme by establishing appropriate policies and procedures, and ensuring their effectiveness. Explicit responsibility should be allocated within the bank for ensuring that the bank's policies and procedures are managed effectively. The procedures for identifying and reporting suspicious transactions to the relevant authorities should be clearly specified in writing, and communicated to all personnel. Banks should establish internal procedures for assessing whether the bank's statutory obligations under the Banking Act require the transaction to be reported to the relevant authorities.

37. Banks' internal audit plays an important role in independently evaluating the risk management and controls, through periodic evaluations of the effectiveness of compliance with KYC policies and procedures, including related staff training. The BSS expects that a bank's compliance function

should provide an independent evaluation of the bank's own policies and procedures, including legal and regulatory requirements. Its responsibilities should include ongoing monitoring of staff performance through sample testing of compliance and review of exception reports to alert senior management, the Board of Directors or, in the case of foreign bank branches appropriate officers outside South Sudan, if it believes management is failing to address KYC procedures in a responsible manner.

38. Banks are required to have an ongoing employee training programme so that bank employees are adequately trained in KYC procedures. Banks should put in place training policies, procedures and other measures to ensure that employees are aware of domestic laws and regulations relating to money laundering and the financing of terrorism. Regular refresher training should be provided to ensure that staff are reminded of their responsibilities and are kept informed of new developments.

39. External auditors also have an important role to play in monitoring banks' internal controls and procedures, and in confirming that they are in compliance with supervisory practice. In terms of Section 90 of the Banking Act banks' external auditors have obligations to report to the BSS if during the review the auditor is of the opinion that a criminal offence has been committed or the interests of depositors and creditors have been jeopardized.

XI. Reporting to the Bank of South Sudan

40. From the date of this Circular, identification documents for all newly opened accounts held at all licensed banks in South Sudan must conform at least with the minimum requirements set out in this Circular. For all accounts opened prior to the date of this Circular, the necessary identification documents must be updated to meet the minimum required standard within three months from the date of this Circular.

41. With effect from the date of this Circular, all banks shall report weekly to the BSS, Supervision Department not later than the end of the next business day (weekly reporting form – Appendix A), the following:

    a. all cash transaction above USD 10,000 or equivalent in SSP or in any other currencies;

    b. all non-cash transactions above USD 20,000 or equivalent in SSP or in any other currencies;

    c. all foreign currency transactions above USD 10,000 (US dollars ten thousand) or equivalent in other foreign currencies; and

    d. all transactions between the same ordering and receiving customers sum of which exceeds the above mentioned amounts.

42. Until further legislation is introduced or this Circular is amended, all instances listed or described in Sections 16, 17, 18, 27, 35 and 41 of this Circular must be reported to the BSS not later than the end of the next business day following their occurrence.

XII. The role of the Bank of South Sudan

43. The BSS has a responsibility to monitor that banks are applying sound KYC procedures and are sustaining ethical and professional standards on a continuous basis. Under its powers to conduct on-site examinations, provided for under Section 70 of the BSS Act and Section 97 of the Banking Act 2012, the BSS will be seeking to satisfy itself that appropriate internal controls are in place and that banks are in compliance with supervisory and regulatory guidance. The review process will include not only a review of policies and procedures but also a review of customer files and the sampling of some accounts.

Made under my hand on

This 11th day of April 2017

Othom Rago Ajak

Governor
Bank of South Sudan

Appendix A

Reporting bank: _____ (*name of bank*)

Report for: _____ *(date)*

Transactions in SSP* – as per Section 41.a, 41.b and 41.d

S/N	Ordering Customer	Account Number	Cash / transfer	Amount	Beneficiary	Beneficiary's account number	Beneficiary's bank
1							
2							
3							

** All transactions over USD 10,000 equivalent in SSP (cash) and USD 20,000 (bank transfers) equivalent in SSP*

Transactions in foreign currency** (USD equivalent) – as per Section 41.c and 41.d

S/N	Ordering Customer	Account Number	Cash / transfer	Amount	Beneficiary	Beneficiary's account number	Beneficiary's bank
1							
2							
3							

*** All transactions over USD 10,000 (or equivalent)*