

## LEGAL NOTICE NO. 55 OF 2013

**Money Laundering (Accountable Institutions) Guidelines, 2013**

In exercise of the powers conferred upon the Financial Intelligence Unit by section 15(2)(e) of the Money Laundering and Proceeds of Crime Act 2008<sup>1</sup>, I,

**PALESA KHABELE**

Director of the Financial Intelligence Unit, issue the following guidelines:

**Citation and commencement**

1. These guidelines may be cited as the Money Laundering (Accountable Institutions) Guidelines 2013 and shall come into operation on the date of publication in the Gazette.

**Interpretation**

2. In these Guidelines, unless the context otherwise requires, words and expressions used shall have the same meaning respectively assigned to them in the Money Laundering and Proceeds of Crime Act 2008, (hereinafter referred to as “the Act”).

**Responsibilities and accountability**

3. An accountable institution shall establish clear responsibilities and accountabilities to ensure that policies, procedures and controls are in place and maintained to deter criminals from using its facilities for money laundering purposes.

**Compliance officer**

4. (1) An accountable institution shall appoint a compliance officer who shall be the central point of contact with the Sector Supervisory Authority and the Unit.

(2) The Compliance Officer shall be responsible for:

(a) receiving and vetting unusual, suspicious or attempted

suspicious activity reports from staff of the accountable institution;

- (b) filling unusual, suspicious or attempted suspicious reports in all relevant sections of the Suspicious Transactions Reporting Form prescribed under the Act;
- (c) developing an anti-money laundering programme and ensure that it is enforced; and
- (d) coordinating training of staff in anti-money laundering awareness and detection methods, and such other measures for combating money laundering.

### **Procedures**

5. An accountable institution shall -

- (a) establish sufficient procedures for the identification and verification of its customers or clients, as the case may be;
- (b) have procedures for the prompt validation and reporting of unusual, suspicious or attempted suspicious transactions to the Unit;
- (c) provide its Compliance Officer with the necessary access to systems and records to fulfill the responsibilities imposed under these guidelines;
- (d) maintain close cooperation with the Unit and Sector Supervisory Authority;
- (e) make arrangements to verify, on a quarterly basis, compliance with policies, procedures and controls relating to money laundering activities in order to satisfy Sector Supervisory Authorities and the Unit that the requirements to maintain such policies, procedures, and controls have been fulfilled; and
- (f) afford Sector Supervisory Authorities and the Unit suf-

---

efficient access to policy, procedures and control documents relating to money laundering maintained at all reasonable times when so requested.

### **Know Your Customer**

6. (1) An accountable institution shall -
  - (a) satisfy itself that a prospective customer, client or any other person on whose behalf the customer or client is acting is who he or she claims to be; and
  - (b) obtain identification particulars of a customer or a client by reference to a document obtained from a reputable source which bears a clear and easily identifiable photograph.
- (2) A deposit taking accountable institution shall establish clear and consistent policies that deal with procedures and controls in situations where satisfactory evidence of identity cannot be obtained.
- (3) The customer's or client's identity shall comprise:
  - (a) for a natural person:
    - (i) name and surname;
    - (ii) residential address;
    - (iii) citizenship;
    - (iv) copy of passport;
    - (v) telephone number, if any;
    - (vi) occupation and place of work; and
    - (vii) gender;

(b) for a legal entity :

- (i) name;
- (ii) place of incorporation;
- (iii) registered office address;
- (iv) legal status;
- (v) registration or licensing number;
- (vi) directors, secretary and other office bearers;
- (vii) authorized agent; and
- (viii) beneficiaries.

(4) An accountable institution shall -

(a) require the following documents to verify particulars of identity provided on behalf of a legal entity:

- (i) certificate of incorporation or registration;
- (ii) memorandum, if applicable and articles of incorporation;
- (iii) certificate showing the registered office of the legal entity; and
- (iv) particulars of current directors;

(b) obtain and verify -

- (i) particulars of identity of trustees, nominees, or fiduciaries and the underlying beneficiary on whose behalf a business transaction is entered into, and the purpose for which the transaction is entered into shall be established;

- (ii) the identity of the underlying principals, in particular those who are supplying and have control of the property.

(5) A deposit taking accountable institution shall obtain and verify particulars of identity of members and office bearers where transactions are conducted for clubs or society.

(6) For the purposes of this guideline, subguideline (3)(a) shall apply to persons referred to in subguidelines (3)(b)(vi), (vii), (viii), (4)(a)(iv) and (5).

### **Purpose of business relationship**

7. An accountable institution shall -

- (a) obtain a sound knowledge of the purpose for which the customer or client is seeking to establish a business relationship with the accountable institution; and
- (b) report any dealing which appears not to fit the knowledge base for which the business relationship was established.

### **False identity**

8. An accountable institution shall report any customer or client who has established or attempted to establish a business relationship with the accountable institution under a false identity.

### **Customer's income**

9. An accountable institution shall endeavour to make specific checks on the customer's or client's income details to ensure that they are commensurate to the customer's or client's identity details.

### **Account relationship**

10. Where a business relationship is conducted through an account, an accountable institution shall obtain and verify the particulars of the identity of the customer or client at the time the banking or deposit account is opened.

**Once- off relationship**

11. Where a business relationship is conducted on a once- off basis, a deposit taking accountable institution shall obtain and verify the particulars of the identity of the customer or client at the time the transaction occurs, unless the deposit to, or by, the customer or client is less than M20, 000.00.

**Completion and verification**

12. (1) Whenever verification of the customer's or client's identity is satisfactorily completed, further verification shall not be necessary when the customer or client subsequently undertakes transactions as long as regular contact with that customer or client is maintained.

(2) When an existing customer or client closes a business relationship but establishes another business relationship, there shall be no need for verification of the identity of the customer or client unless the business relationship is established after a year or more after closure of the first business relationship.

(3) Where one or more once- off transactions are linked and the deposits together exceed the limit of M20, 000.00, a deposit taking accountable institution shall obtain and verify the particulars of the identity of the customer or client.

(4) A transaction shall not be considered to be linked to another if they are separated by an interval of 3 months or more unless there is specific evidence to the contrary.

**Third parties**

13. A deposit taking accountable institution shall obtain and verify the identity of a third party if the deposit is by, or on behalf of, a third party.

**Power of attorney**

14. (1) A holder of a power of attorney shall be subject to the identity requirements under these guidelines.

(2) An accountable institution shall keep and maintain records of transactions undertaken in accordance with a power of attorney for a period of

not less than 5 years.

### **Internet banking**

15. An accountable institution offering internet banking facilities shall -
- (a) put in place and implement procedures to identify and authenticate the customer;
  - (b) ensure that there is sufficient communication to confirm the address and personal identity of the customer; and
  - (c) monitor, regularly, all accounts opened on the internet and investigate and report attempted or suspicious and unusual transactions.

### **On-going Customer Due Diligence (OCDD)**

16. (1) An accountable institution shall -
- (a) monitor its customers or clients and their transactions on an on-going basis to be called “on-going customer due diligence” or “OCDD”;
  - (b) observe the following OCDD requirements -
    - (i) collection and verification of additional KYC information;
    - (ii) a transaction monitoring programme; and
    - (iii) an “Enhanced Customer Due Diligence” (ECDD) programme;
  - (c) have appropriate risk-based systems and controls based on the nature, size, and complexity of the accountable institution’s business and the money laundering risks faced;

- (d) determine when it may be necessary to collect further KYC information, or update or verify existing KYC information;
- (e) have a transaction monitoring programme to detect complex, unusual large transactions and unusual patterns of transactions, which have no apparent economic or lawful purpose;
- (f) have an ECDD programme immediately upon determining that there is a high money laundering risk, or a suspicious transaction activity has arisen; and
- (g) pay special attention to the particulars of identity and nature of a business transaction of a politically exposed person.

(2) When applying the ECDD programme referred to in subguideline (1)(f), an accountable institution shall consider issues such as whether to analyze, verify, re-verify, update, or obtain any KYC information about a customer or client, analyze and monitor the customer's transactions, clarify the nature of the customer's or client's on-going business with the accountable institution, or report a suspicious transaction to the Unit.

### **Record keeping**

17. (1) An accountable institution shall keep and maintain the following records of its customers or clients' business transactions for a period of five (5) or more years beginning on the date a business transaction is conducted and ensure that they are readily available as required under the Act:

- (a) daily records of transactions;
- (b) receipts;
- (c) paying-in books;
- (d) customer or client correspondence; and
- (e) cheques.



- 
- (2) Records of transactions shall be kept either in hard or electronic form.
- (3) An accountable institution shall ensure that -
- (a) documents kept centrally are distinguishable between transactions relating to different customers in their form and content;
  - (b) records of suspicions are not inappropriately disclosed to the client or third party to avoid offences of tipping off and prejudicing an investigation;
  - (c) the following documents and records are kept:
    - (i) documents used to verify identity of the customer or client;
    - (ii) supporting evidence and records showing a business transaction or service;
    - (iii) documents or information used to verify the identity of a beneficial owner;
    - (iv) information on purpose and the intended nature of the business relationship with the customer or client;
    - (v) records of on-going monitoring;
    - (vi) documents or information on politically exposed persons;
    - (vii) documents or information on correspondent banking relationships;
    - (viii) documentation on reliance on third parties;
    - (ix) records of decisions made on risk policy and risk based approach applied;

- (x) records of decisions made on veracity or adequacy of previously obtained documents;
- (xi) records of evidence of training and compliance monitoring;
- (xii) records of decisions on filling of, or failure to fill, suspicious transaction reports; and
- (xiii) annual and other reports on the designated persons on anti-money laundering systems and controls.

### **Recognition of suspicious activities or transactions**

18. (1) In these guidelines where there is a business relationship, a suspicious transaction may be one which is inconsistent with a customer's or client's known, legitimate business or personal activities or with the normal business activity of that type of account.

(2) An accountable institution shall, as far as practicable, endeavour to know enough of its customers or clients and their business to recognise that a transaction or a series of transactions is unusual.

(3) For purposes of these guidelines, an accountable institution shall, among others, consider the indicators or the questions in the Schedule to determine whether a customer's or client's transaction or activity is suspicious or not.

### **Reporting of suspicious transactions**

19. (1) An accountable institution shall, through its Compliance Officer, report suspicions of money laundering to the Unit.

(2) Upon receipt of a suspicious transaction from an employee of an accountable institution, the Compliance Officer shall, on behalf of the accountable institution, report the suspicious transaction or activity to the Unit in the Suspicious Transactions Reporting Form obtainable in both hard and electronic form at the offices of the Unit, Central Bank of Lesotho Building and a completed Suspicious Transactions Reporting Form shall be submitted, at least, within a period of 7 days of forming a suspicion.

(3) Sufficient information shall be disclosed which indicates the nature of and reason for the suspicion and where an accountable institution has additional documentation in relation to the suspicion, that documentation shall be made available.

(4) A compliance officer shall -

- (a) act honestly and reasonably in making determinations on whether the customer or client is engaged in money laundering and submit the report in good faith;
- (b) determine whether the information or matters contained in the transaction report give rise to a knowledge or suspicion that a customer or client is engaged in money laundering and in making this determination, the Compliance Officer shall consider all relevant information available within the accountable institution, and any other available sources concerning the customer or client.

(5) An accountable institution shall ensure that all employees dealing with customers or clients know that they are obliged to report suspicious transactions or activities to the Compliance Officer.

(6) An accountable institution shall ensure that -

- (a) internal reporting lines are kept as short as possible, with the minimum number of people between the person who has developed a suspicion about a particular transaction and the Compliance Officer to ensure speed and confidentiality when reporting; and
- (b) no obstacles are placed in the way of the reporting of suspicions developed by their staff to the Compliance Officer.

(7) All suspicions reported to the Compliance Officers, and all internal inquiries made in relation to the suspicions, and the reason behind whether or not to submit the suspicious transaction or activity report shall be documented by the responsible person at the accountable institution.

(8) A compliance officer shall endeavour to submit a suspicious transaction or activity report after undertaking reasonable internal enquiries to determine that all available information has been taken into consideration and not as a matter of routine.

(9) An accountable institution may not receive feedback on the state of an investigation if the investigation is of a confidential nature or if the matter is *sub judice*.

(10) A compliance officer may be contacted to provide supplementary information after the Compliance Officer has submitted the suspicious transaction or activity report.

#### **Termination of a business relationship after reporting**

20. An accountable institution wishing to terminate a business relationship with a customer or client after disclosure of a suspicious transaction or activity by the customer or the client shall ensure that the termination does not in any way “tip-off” the customer or the client and prejudice the investigations.

#### **Education and training**

21. (1) An accountable institution shall -
- (a) establish a training programme designed to ensure that employees are aware of money laundering transactions and are aware of their obligations to report suspicious transactions or activities;
  - (b) develop manuals and training programmes to ensure that employees are aware of their responsibilities;
  - (c) ensure that employees are educated on the importance of the “Know Your Customer” (KYC) requirements for money laundering prevention purposes; and
  - (d) ensure that employees, when a business relationship is established, know enough about the type of business activities expected in relation to the customer or client from the onset to know what may constitute a suspicious

transaction or activity at a future date.

(2) A general appreciation of the background to money laundering and the subsequent need for reporting of any suspicious transaction or activity to the Compliance Officer shall be provided to all new employees who will be dealing with customers or clients irrespective of the level of seniority.

(3) An accountable institution shall take measures to ensure that a new employee is made aware of the legal requirement of reporting suspicious transactions or activities.

(4) Training shall be provided for on factors and new trends on money laundering techniques that may give rise to suspicions and on the procedures to be followed when the transaction is considered suspicious.

(5) An employee who is in the process of establishing a business relationship with a new customer or client shall be made aware of the need to identify the customer and verify the identity information supplied by the customer or client or any party acting on behalf of the customer or client.

(6) An employee who processes the settlement of bargains shall receive appropriate training in the processing and verification procedures and in the recognition of abnormal settlement, payment or delivery instructions.

(7) Training covering all aspects of money laundering control procedure shall be provided to those with the responsibility for supervising or managing employees, as well as audit and compliance officers responsible for the review of procedures used by accountable institutions to deal with faults or weaknesses in systems or procedures used by accountable institutions.

(8) An accountable institution shall ensure that refresher training at regular intervals is conducted to ensure that employees do not forget their responsibilities.

(9) Training for money laundering purposes shall be tailored to meet the needs of the particular accountable institution.

### **Failure to comply**

22. Failure to comply with these guidelines shall be punishable by an ad-

ministrative sanction to be imposed by Sector Supervisory Authorities and the Unit.

### **Sanctions**

23. A sector supervisory authorities or the Unit may, by written notice, impose an administrative penalty not exceeding M20, 000.00 on an accountable institution, its directors, employees or agents for non-compliance with these guidelines or any sanctions provided for by law under which the accountable institution is established and registered.

**PALESA KHABELE**  
**DIRECTOR, FINANCIAL INTELLIGENCE UNIT**

### **NOTE**

1. Act No. 4 of 2008

## SCHEDULE

(guideline 18(3))

## INDICATORS OF SUSPICIOUS TRANSACTIONS

**Indicators and questions to determine whether a customer's or client's transaction or activity is suspicious or not. These indicators may not always be immediately indicative of a suspicious transaction or activity but may give rise to further monitoring and due diligence.**

1. Is the size of the transaction consistent with the normal activities of the customer or client? Unusually large cash transactions made by an individual or company whose ostensible business activities would normally be generated by cheques and other instruments.
2. Is the transaction rational in the context of the customer or client's business or personal activities? Substantial increases in cash deposits of any individual or business without apparent cause, especially if such deposits are subsequently transferred within a short period out of the account and to a destination not normally associated with the customer.
3. Has the pattern of transactions conducted by the customer or client changed?
4. Where the transaction is international in nature, and the customer or client is based overseas, does the customer or client have any obvious reason for conducting business in Lesotho? If the customer or client is based in Lesotho, is there any obvious reason for the customer or client conducting business overseas?
5. Customers whose deposits contain counterfeit notes or forged instruments.
6. Customers who seek to exchange large quantities of low denominations notes for those of higher denominations.
7. Frequent exchange of cash into other currencies without good reason.
8. Customers transferring large sums of money to or from overseas locations with instructions for payment in cash.

9. Customers who have numerous accounts and pay in amounts of cash to each of them in circumstances in which the total of credits would be a large amount.
10. Any individual or company whose account shows virtually no normal personal banking or business related activities, but is used to receive or disburse large sums which have no obvious purpose or relationship to the account holder or his business (e.g. a substantial increase in turnover on an account).
11. Reluctance to provide normal information when establishing a business relationship, providing minimal or fictional information or, providing information that is difficult or expensive for an Accountable Institution to verify.
12. Paying in large third party cheques endorsed in favour of the customer or client.
13. Large cash withdrawals from a previously dormant or inactive account or from an account which has just received an unexpected large credit from abroad.
14. Substantial increases in deposits of cash or negotiable instruments by a professional firm or company, using client accounts or in-house company or trust accounts, especially if the deposits are promptly transferred between other client company and trust accounts.
15. Large number of individuals making payments into the same account without an adequate explanation.
16. Customers who request that account statements and other correspondence be kept at the Accountable Institution for collection or from whom correspondence is returned marked "not known at this address" etc.
17. Frequent requests for travellers cheques, foreign currency drafts or other negotiable instruments to be issued that are not consistent with known customer profile.
18. Changes in employee characteristics, including but not limited to lavish life styles.



- 
19. Customers of casinos who request that payouts be sent to third parties, particularly in jurisdictions of not their domicile.
  20. Customers of casinos who deposit significant sums into their player accounts and then withdraw the money without having undertaken much gaming activity.
  21. Multiple loans obtained over a short period of time with repayments made in cash by either the contract owner or third parties
  22. Multiple transactions of a similar nature on the same day in different locations.
  23. Purchasing high value assets including but not limited to movable and immovable property followed by immediate resale with payment requested via cheque.
  24. Physical removal of large cash or negotiable instruments out of the country.
  25. Third party present for all transactions but does not participate in the actual transaction.
  26. Use of an intermediary to make insurance policy payments.
  27. Unusual large transfer of money from an individual to a business.
  28. Use of gatekeepers including but not limited to accountants or lawyers to undertake transactions.
  29. "U-turn" transactions occurring with funds being transferred out of the country and then portions of those funds returned.
  30. Investment cheques issued to a family member.
  31. Frequent early repayments of loans.
  32. Large cash deposits used for investments.
  33. Large amounts of currency exchanged for travelers cheques.

34. Frequent transfers indicated as loans sent from relatives.
35. Wire transfers to and from tax haven countries including but not limited to Vanuatu and British Virgin Islands.