RESERVE BANK OF ZIMBABWE

Guideline No. 01 – 2002 / BSD

ANTI-MONEY LAUNDERING GUIDELINES FOR BANKING INSTITUTIONS

1. BACKGROUND

Money laundering refers to the use of banking and other financial institutions, and any other institutions in the deposit and transfer of funds derived from criminal activity. Criminals launder money in order to disguise the identity of its source. Rapid technological advancement and the increased integration of the world's financial systems have enhanced the ease with which criminal money can be laundered. On the other hand, the identification and tracing processes have been complicated.

Countries throughout the world are setting up frameworks that enable them to prevent criminals whenever possible, from legitimizing the proceeds of their criminal activities by cleaning up 'dirty' money via the financial system, as well as detect terrorist financing. Money laundering must be curbed because it provides the fuel for criminal activity including terrorism.

1.1 The Money Laundering Process

The traditional money laundering process basically involves three independent steps that often occur simultaneously.

1. Placement stage

The launderer introduces his illegal profits into the financial system. This can be achieved by breaking up large amounts of cash into less conspicuous smaller sums that are then deposited with banks, or by purchasing monetary instruments such as money orders, that are then collected and deposited into accounts at another location.

2. Layering stage

The launderer engages in a series of conversions or movements of the funds to distance them from their source. The launderer creates complex layers of financial transactions designed to disguise the audit trail and provide anonymity. This might be done through the purchase and sale of investment instruments. In some instances, transfers may be disguised as payments for goods and services, thus giving the funds a legitimate appearance.

3. Integration

The funds re-enter the legitimate economy. The launderer may invest the funds into real estate, business ventures or other investments.

Today money laundering methods have become more complex and subtle involving the less obvious organizations such as legal and accounting firms, estate agents, dealers in high value goods and others. This calls for vigilance on the part of all organizations that are potentially vulnerable to money laundering and related criminal activity. The financial system is at the heart of anti-money laundering efforts because money laundering is basically a financial crime.

1.2 Terrorist financing

While financial gain is generally the objective of other types of criminal activity, the primary objective of terrorism is to intimidate target persons, organizations or governments. Terrorist organizations however still require financial support to accomplish their activities and accordingly, financial institutions may be used to deposit and transfer funds. It is for this reason that all banking

institutions are called upon to be on the look out for transactions that are related to terrorist financing.

1.3 Banking institutions and the control of money laundering activities

In order to control money laundering and related criminal activities, money launderers should not be allowed to enjoy the profits arising from their criminal activities. Similarly, terrorist organizations should be prevented from accessing the financial support they require to carry out their criminal activities.

The Reserve Bank, as the supervisory authority for banking institutions, is concerned with the possible use of banking institutions by money launderers and other criminals. The primary objective of banking supervision is to promote and maintain a safe and sound banking system and to ensure financial stability. Banking business is dependent to a great extent on public confidence. Banking institutions should therefore guard against abuse of their organizations by money launderers as this undermines the integrity of their institutions, and hence public confidence in the individual institutions as well as the banking system as a whole.

The Reserve Bank has prepared minimum criteria and standards for banking institutions in the fight against money laundering.

2. INTERNAL CONTROLS, POLICIES AND PROCEDURES

The Banking Act (Chapter 24:20) requires every banking institution to establish adequate internal control systems, information systems, and appropriate accounting procedures and accounting controls, in respect of their banking business. (*Reference: Sections 16, 17, and 40*)

Banking institutions should also establish clear responsibilities and accountabilities to ensure that policies, procedures and controls which deter criminals from using their facilities for money laundering, are followed and maintained.

Banking institutions are thus required to verify on a regular basis, compliance with policies, procedures and controls relating to money laundering to satisfy bank management that the laid down requirements have been discharged.

3. CHARACTERISTICS OF SUSPICIOUS TRANSACTIONS / ACTIVITIES

Banking institutions should have the ability to assess transactions according to the circumstances on hand to determine whether a transaction is suspicious or otherwise. Suspicion could be based on the size of transaction or amount of cash involved, or the circumstances of the transaction.

Banking institutions should be alert to changes in bank transactions, unusual characteristics or activities, attempts to avoid record keeping requirements, provision of insufficient or suspicious information. *Annexure 1* provides examples of what may constitute suspicious transactions.

4. GENERAL GUIDELINES

Banking institutions should make a reasonable effort to determine the true identity of all customers requesting their services. They should never open an account or conduct business with a customer who insists on anonymity or ‘‘bearer’’ status, or who gives a fictitious name. Banks should never enter a business relationship until the identity of a new customer is satisfactorily established. The owners of all accounts and of those using the safe custody facilities should be clearly identified.

Whenever an account is to be opened with a banking institution, or a significant one-off transaction or series of linked transactions undertaken, the identity of the prospective customer must be verified.

The requirement to verify identity applies to :

- new business relationships,
- existing relationships if the relationship is to continue after the effective date of the guidelines, and
- significant one-off transactions or series of linked transactions (> $500 000).

Once identification procedures have been satisfactorily completed, then the business relationship has been established, and as long as records are maintained in line with Section 37 of the Banking Act, and the requirements of these Guidelines, no further evidence of identity is needed when transactions are subsequently undertaken, unless it is deemed necessary.

Exemptions

Steps to verify identity are not required in the following circumstances :-

- Where the applicant is a Zimbabwean banking institution, and
- One-off transactions single or linked (occasional customers) under $500 000, unless money laundering is suspected or known to have or to be taking place.

Policies and procedures

- Every banking institution should develop policies and procedures that enable the institution to detect, prevent and report suspicious transactions.

- Banking institutions should have adequate information systems capable of monitoring customer accounts and thereby enabling proactive account monitoring for suspicious activities.

KNOW-YOUR-CUSTOMER PROGRAMS

- Banking institutions should deal with customers they ‘know’. In this regard every banking institution shall establish a comprehensive Know-Your-Customer (KYC) program. The KYC program should include policies and procedures for customer acceptance, customer identification, ongoing review and monitoring of accounts and risk management.

- The KYC procedures should enable the banking institution to collect sufficient information to develop a customer profile that will enable the institution to realistically determine when transactions are suspicious or potentially illegal.

- The banking institution’s board of directors should be fully committed to an effective KYC program embracing policies and procedures for proper management oversight, systems and

controls, segregation of duties, training and other related policies, including procedure for handling suspicious transactions.

Customer Acceptance Policy

- Banking institutions should develop and document clear customer acceptance policies and procedures, including a description of customers that should not be permitted to open accounts. A tiered customer identification program should be employed, that involves more extensive due diligence for higher risk accounts.

Business relationships

- A banking institution should establish to its satisfaction that it is dealing with a real person (natural or legal). Whenever the identity of the beneficial owner(s) of an account cannot be ascertained, the banking institution shall deny or close such an account.

- Banking institutions need to be vigilant in preventing corporate business entities from being used by natural persons to launder funds. In this regard banking institutions should carefully understand the structure of companies, their sources of funds, and identify the beneficial owners and those who have control over the funds.

- Decisions to enter into business relationships with individuals holding important public positions, or insiders as defined by the Banking Regulations, should be taken at senior management level. Banks should be particularly vigilant with respect to monitoring such accounts, as they may expose the bank to significant reputational and/or legal risks when the persons involved are corrupt.

Minimum standards for vetting

- Banking institutions shall take reasonable measures to obtain, record and maintain current information about the true identity of the person on whose behalf an account is opened or a transaction is conducted, if there are any doubts that a client is acting on their own behalf.

- Banking institutions shall obtain and keep up-to-date customer identification papers and retain them for at least *six years* after an account is closed.

Records retention

- All financial transaction records shall be retained in both electronic form and hard copy for at least *six years* after the transaction has taken place. The records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved if any) so as to provide, if necessary, evidence for prosecution of criminal behaviour.

5. SPECIFIC GUIDELINES

The following guidelines shall be the minimum requirements to be complied with by every banking institution.

5.1 ACCOUNT OPENING FOR PERSONAL CUSTOMERS

The following information should be obtained from prospective customers :-

- ✓ True name and / or the names used.

- ✓ Permanent address, this can be done by requesting sight of a recent utility bill, local authority bill or a bank statement. In addition the banking institution can also perform a telephone directory search.
- ✓ Date of birth.

Ideally the true name should be verified by reference to a document obtained from a reputable source which bears a photograph.

It should however be noted that no single form of identification can be fully guaranteed as representing correct identity. The identification process will therefore generally need to be cumulative and performed to the satisfaction of the banking institution providing the service.

A person's address is an essential part of identity. Verification of the current permanent address of the prospective customer is therefore required.

The above identification process is additional to industry initiatives such as the services offered by the Financial Clearing Bureau.

5.1.1 Acceptable Identification documents and/or particulars

Zimbabwean Citizens

- National identity card
- Valid Passport
- Zimbabwean Driver's licence

Foreigners

- Valid passport

5.1.2 Account opening for students and young people

The normal identification procedures set out above should be followed as far as possible. Verification may also be obtained via the parents or guardians of the applicant customer, or by making enquiries at the college or university.

5.1.3 Confirmation of identity by other banking institutions

The primary duty to verify identity using the best evidence and means available rests with the account opening institution. However, where a banking institution cannot obtain verification of identity of a potential customer with satisfaction, they may approach another banking institution where the customer has or had an account on a non-competitive basis, specifically for the purpose of verifying identity. It is extremely important that all banking institutions respond to such requests without undue delay. *The requests should only be made if verification cannot be obtained from other sources.*

5.2 ACCOUNT OPENING FOR CORPORATE CUSTOMERS

The following documents should be obtained :-

- o The original or certified copy of the certificate of incorporation,
- o The memorandum and articles of association, and
- o The resolution of the board of directors to open an account and confer authority on those who will operate it.

A search of the company's file at the Companies Registration Office should be conducted in order to verify the information provided and authenticity of the documents submitted.

5.3 ACCOUNT OPENING FOR CLUBS, SOCIETIES, CHARITIES

The banking institution should satisfy itself as to the legitimate purpose of the organization by, for example, requesting sight of the constitution.

The identities of all the signatories to the account should be verified.

5.4 UNINCORPORATED BUSINESSES

Where a formal partnership arrangement exists, a mandate from the partnership authorizing the opening of an account and conferring authority on those who will operate it, should be obtained.

The partnership contract should be called for as an identification document.

In all other cases, the identities of at least two partners should be verified in line with the requirements for personal customers.

5.5 TRUST AND SIMILAR ACCOUNTS

When it is known or suspected that an account is being opened, or a transaction is being undertaken on behalf of a third party without the name of that third party being disclosed, the banking institution must obtain information on the identity of the person on whose behalf the customer is acting. If the principals cannot be identified, the account should be denied.

Where the banking institution has no current relationship with a proposed trustee, verification of identity of the trustee(s) should be undertaken in line with normal procedures outlined above for personal customers.

Where money is received by a trust, the banking institution should ensure that the source of the money is properly identified, the nature of the transaction is understood, and payments are made only in accordance with the terms of the trust and are properly authorized in writing.

The affairs of a trust must be properly documented.

Where a nominee opening an account on behalf of another person is not already known to the banking institution, the identity of the nominee or any other person who will have control of the account should be verified.

A GENERAL NOTE ON NON-PERSONAL CUSTOMERS

When dealing with entities, the banking institution should be able to :-

- identify and verify the identity (documents and information) of the direct customer,
- identify the person(s) with beneficial ownership and control,
- verify the identity of the beneficial owner and/or the person on whose behalf a transaction is being conducted.

6. AREAS REQUIRING SPECIAL MENTION

6.1 INTRODUCED BUSINESS

Where business is being referred, the recipient bank may rely on the identification and verification procedures of the referring bank or introducer only when the bank is satisfied with the integrity of the introducer and has ascertained that the introducer is exercising the necessary due diligence called for by these guidelines, and any other best practice standards. The following criteria should be applied in determining whether an introducer can be relied upon :-

- The introducer must comply with the minimum customer due diligence practices outlined in these guidelines.
- The customer due diligence procedures of the introducer should be as rigorous as those that the bank would have conducted itself for the customer.
- The banking institution must satisfy itself as to the reliability of the systems put in place by the introducer to verify the identity of the customer.
- It must be possible for the banking institution to verify at any stage, the due diligence undertaken by the introducer.
- The banking institution must immediately receive from the introducer and review, all relevant identification and other documentation pertaining to the customer's identity.

The overall identification and verification procedure is the ultimate responsibility of the banking institution entering into the business relationship with the customer.

6.2 INTERNET BANKING

Banking institutions are prohibited from opening accounts via the Internet or through the post.

Internet banking services should be made available only to a customer who has an account with the banking institution or another banking institution, and whose identity has been verified.

6.3 CORRESPONDENT BANKING

Banking institutions should be able to apply a satisfactory level of due diligence to correspondent accounts to prevent their institutions from being used by criminals to transmit money linked to criminal activity. Some of the factors to consider include :

- Location of the respondent bank and the standard of bank regulation and supervision in that jurisdiction,
- The respondent bank's risk management processes including anti-money laundering measures.
- The purpose of the account.
- The identity of any third party entities that will use the correspondent banking services.

6.4 CLIENT ACCOUNTS OPENED BY PROFESSIONAL INTERMEDIARIES

Where a professional intermediary opens an account on behalf of a single client, that client must be identified.

In the case of pooled accounts :

(i) Where sub-accounts attributable to each beneficial owner exist, banking institutions must identify all the beneficial owners of the account held by the intermediary,

(ii) Where the funds are co-mingled, and where the intermediary is subject to the same due diligence standards as the banking institution, reliance may be placed on the

intermediary if the banking institution is satisfied that the intermediary has the capacity to and has performed the necessary due diligence procedures. If these conditions cannot be satisfied, the intermediary account should be denied.

7. REPORTING REQUIREMENTS

The relevant authorities in Zimbabwe are working towards the establishment of a Financial Intelligence Unit that will have the responsibility of receiving suspicious transaction reports as well as coordinating the country's anti-money laundering efforts.

Until such time that a Financial Intelligence Unit is established, banking institutions shall report suspicious transactions to the Banking Supervision Department in the Reserve Bank of Zimbabwe. This does not, however, preclude banking institutions from fulfilling their obligations under other laws.

When to make a report

- All suspicious transactions that involve potential money laundering and the financing of terrorism regardless of the amount of money involved.
- Insider abuse involving any amount.
- All cash transactions aggregating $500 000 (five hundred thousand dollars) or more.
- Where the banking institution has chosen not to enter into a business relationship or a transaction that they suspected to be linked with money laundering or the financing of terrorism.

  * The threshold of $500 000 (five hundred thousand dollars) is subject to review by Banking Supervision in line with current market practices, prevailing inflation levels and any other relevant factors.

Frequency of reporting

Where immediate action is required, a banking institution shall immediately notify the appropriate law enforcement agency and Banking Supervision Department in the Reserve Bank of Zimbabwe. In addition, every banking institution shall file on a monthly basis, a summary of the suspicious transactions. The report should reach Banking Supervision Department no later than the 5th of the following month. (*See Annexure 2 for the minimum contents of the report.)*

8. HANDLING OF SUSPICIOUS TRANSACTIONS AND COMPLIANCE RESPONSIBILITY

Every banking institution shall appoint a Money Laundering Reporting Officer as well as a deputy or an alternate to act in his absence. The Money Laundering Reporting Officer may have other duties depending on the particular circumstances of the institution. He should be sufficiently senior to command the necessary authority, since he is the reference point in the organization, as well as the interface with the outside law enforcement and supervisory authorities.

Banking institutions are not allowed to inform their clients when information relating to them is being reported to competent authorities.

All banking institutions must ensure that :-

- Each relevant employee knows to which officer in the banking institution they should report suspicious transactions, and
- There is a clear reporting chain under which the suspicious transactions will be passed without delay to the Reporting Officer.

The role of the Money Laundering Reporting Officer

The Money Laundering Reporting Officer is the compliance contact person, with day-to-day responsibility for the compliance program. He is required to determine, inter alia, whether the information contained in the transaction report he has received, gives rise to a knowledge or suspicion that a customer is engaged in money laundering activities and/or the financing of terrorism. In making his judgment he should consider all other relevant information within the banking institution concerning the customer to which the report relates. This may include a review of other transaction patterns and volumes through the customer's account(s), the length of the business relationship, etc.

9. EDUCATION AND TRAINING PROGRAMS

Every banking institution should ensure on an going basis, that staff undergo education and training programs that enable them to effectively identify and handle transactions relating to known or suspected cases of money laundering.

The content of training programmes will differ according to institutional needs. There is need for continuous and updated training to ensure personnel is provided with the most current and up to date information. The following coverage for a training program is recommended at a minimum.

a) New Employees

- ✓ A general appreciation of the background to money laundering and the need for reporting of any suspicious transactions to the money laundering reporting officer.
- ✓ The importance of reporting, and the legal or otherwise obligations of the bank and individual officers.
- ✓ Issues of protection of staff who report suspicious transactions.

b) The Money Laundering Reporting Officer.

- o In depth training concerning all aspects of the legislation, regulations and internal policies.
- o Extensive initial and ongoing instruction on the validation and reporting of suspicious transactions.

c) Cashiers/ Foreign Exchange Officers / Advisory Staff and other customer contact personnel

These members of staff deal directly with the public and are therefore the first point of contact with potential money launderers. They should be well trained on factors that may give rise to suspicions and on the procedures to be adopted when a transaction is deemed suspicious.

d) Account Opening / New Customer Personnel

In addition to the training that is given to the cashiers, this group should also receive training relating to the need to verify the identity of the customer, as well as training in the organisation's account opening and customer / client verification procedures.

e) Administration / Internal Audit / Operations Supervisors and Managers
This group of people should receive training concerning all aspects of money laundering procedures including the legal position, internal reporting procedures, and the requirements for verification of identity and the retention of records.

10. REMEDIAL MEASURES /ADMINISTRATIVE SANCTIONS

If a banking institution fails to comply with these Guidelines, the Reserve Bank may pursue any remedial measures at its disposal in terms of Section 48 of the Banking Act.

11. COVERAGE AND EFFECTIVE DATE

These guidelines cover all types of banking business and are effective from 1st November 2002.

Questions relating to these guidelines should be addressed to the Deputy Director, Supervision and Surveillance, Reserve Bank of Zimbabwe, Telephone 703 000 extension 11133.

_____

S. Gwasira
Director, Supervision and Surveillance

Annexure 1

EXAMPLES OF SUSPICIOUS TRANSACTIONS / ACTIVITIES

Unusual characteristics or activities and changes in bank transactions

- Cash deposits relating to transactions that would normally be settled by cheque. For example corporate accounts where deposits or withdrawals are primarily in cash rather than cheques.
- Request to exchange large quantities of low denominations for higher denominations.
- Requests for cheque clearance of large sums.
- Matching payments out with credits paid in by cash on the same or previous day.
- Significant turnover in large denomination bills uncharacteristic for the bank's (or branch's) location.
- Rapid increase in size and frequency of cash deposits without any corresponding increase in non-cash deposits.
- A customer who suddenly pays up a large problem loan with no reasonable explanation of the source of funds.
- A depositor who purchases money orders with large amounts of cash.
- Mixing of cash deposits and monetary instruments in an account which such transactions do not appear to have any relation to the normal use of the account.
- Where the customer's stated purpose for a loan does not make economic sense.
- A dormant account containing a minimal sum suddenly receives a deposit or series of deposits followed by daily cash withdrawals running down the transferred amount.
- An account for which several persons are signatories, yet the persons appear to have no relation among each other (either family ties or business relationship).
- The opening by the same person of multiple accounts into which numerous small deposits are made that in aggregate are not commensurate with the expected income of the customer.
- *Non- profit or charitable organizations* - Financial transactions for which there appears to be no link between the stated activity of the organisation and the other parties in the transaction.

Funds transfer activities

- The sending or receipt of frequent or large volumes of wire transfers to and from offshore institutions
- Customers transferring large sums of money to or from overseas with specific requests for payment in cash.
- International transfers for accounts with no history of such transfers or where the stated business of the customer does not warrant such activity.
- Significant changes in currency shipment patterns between correspondent banks.
- Deposits that are followed within a short time by wire transfers of funds to or through a location of specific concern , such as a country with lax controls

Insufficient or suspicious information

- A business that is reluctant to provide complete information regarding the purpose of the business or details of business activities, prior banking relationships, directors, or the location of the business.
- A business that is reluctant to provide details about its activities or to provide financial statements.
- A business that provides financial statements that are noticeably different from those of similar businesses.

- A customer who is unwilling to provide personal background information.
- A customer who has no record of past or present employment on a loan application.
- A customer who has no record of past or present employment but makes frequent large transactions.

Attempts to avoid reporting or record keeping requirements

- A customer who is reluctant to provide information required for identification, and record keeping purposes.
- A customer who does not give details on record of past or present employment on a loan application form.
- A customer who attempts to coerce a bank employee to not file required record keeping or reporting forms.
- A customer who requests for exemption from reporting or other requirements.
- The deposit or withdrawal of cash in amounts which fall consistently just below identification or reporting thresholds.

Banking institution employees

- An employee whose lavish lifestyle cannot be supported by his salary.
- Reluctance by an employee to take a vacation.
- Mysterious disappearances or unexplained shortages of significant amounts of bank funds.

The above list is not intended to be all inclusive.

Annexure 2

MINIMUM CONTENTS OF SUSPICIOUS TRANSACTION / ACTIVITY REPORT

1. Reporting Banking Institution Information
Name and address of institution
Name and address of Branch where the activity occurred

2. Suspect Information
Full Names or Name of Entity
Address
Phone Number - Residence
- Work
Occupation / Type of business
Date of birth

Forms of identification - National registration number
- Valid Passport Number
- Zimbabwean Driver's Licence
Relationship to financial institution (Employee, Director, Officer, Shareholder, Customer etc.)

3. Description of the suspicious activity
Type of transaction
Amount involved
Other details necessary to understand the transaction

4. Action already taken
- If an insider is involved what action has been taken?
- Has any law enforcement agency been advised? If yes, provide name of agency, name and telephone number of person(s) contacted, and by what method (telephone, written communication, etc)

5. Contact person
Full names
Title / Designation
Contact telephone number

6. Date of suspicious transaction and date of preparation of report