RESERVE BANK OF MALAWI

DIRECTIVE

NO.DO1-2005/CDD

CUSTOMER DUE DILIGENCE FOR BANKS AND FINANCIAL INSTITUTIONS

Arrangement of Sections

Inspection by the Reserve Bank

SECTION

PART VII

Remedial Measures and Administrative Sanctions

SECTION

PART VIII

Effective Date

SECTION

PART I: SHORT TITLE, AUTHORIZATION, APPLICATION AND INTERPRETATION

Sec. 1: Short Title – Customer Due Diligence

Sec. 2: Authorization – Sections 26, 28, 38, 47 and 49 of the Banking Act of 1989;

Sec. 3: Application – All Banks and Financial Institutions licensed to conduct banking business in Malawi

Sec. 4: Interpretation - In this Directive unless the context otherwise requires

1) "account" means any facility or arrangement by which a bank or financial institution does any of the following:
   (a) accepts deposits;
   (b) allows withdrawals; or
   (c) pays cheques or payment orders drawn on the bank or financial institution, or collects cheques or payment orders on behalf of a person other than the financial institution;
   and includes any facility or arrangement for a safe deposit box .

2) "bank" is as defined in Section 2 of the Banking Act of 1989;

3) "cash" means any coin or paper money that is designated as legal tender in the country of issue and includes bearer bonds, travellers' cheques, postal notes and money orders.

4) "customer" any person or entity who has an account with a bank or financial institution involving the receipt or disbursal of funds and shall include any person or entity on behalf of who an account is maintained.

5) "financial institution" is as defined in Section 2 of the Banking Act of 1989 but shall also include money transmission service providers.

6) "Financial crime**"** means any crime that generally results in a pecuniary loss, including financial fraud regardless of the intention or whether violence was involved.

7) "Integration" means the turning of criminally derived wealth into 'legitimate' funds.

8) "Layering" means separating illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the audit trail and provide anonymity.

9) "Placement" means the process of placing unlawful proceeds into financial institutions through deposits, wire transfers or other means.

10) "Proceeds of crime" means any money or property that is derived or realised, directly or indirectly, by any person from the commission of an offence.

PART II: STATEMENT OF POLICY

Sec. 1: Objectives

1) To ensure that banks and financial institutions establish and regularly maintain policies, practices and procedures designed to determine the true identity of their customers as well as their customers' normal and expected transactions and sources of funds.

2) To facilitate banks' and financial institutions' compliance with the Banking Act, 1989 and with safe and sound banking practices so as to maintain the integrity of the financial sector.

3) To protect banks and financial institutions from becoming vehicles for, or victims, of illegal activities, including money laundering, perpetrated by their customers.

4) To foster cooperation amongst banks and financial institutions in customer identification and the on-going monitoring of suspicious accounts and transactions.

5) To ensure that the financial sector (and the nation) complies with international conventions and initiatives by international bodies (eg the United Nations, Basle Committee on Banking Supervision and the Financial Action Task Force) in the prevention of the criminal use of the financial system.

6) To ensure that all banks and financial institutions uphold the same standards so as to level the playing field between institutions that have already adopted formal Know Your Customer (hereinafter referred to as KYC) principles and those that have not yet done so.

Sec. 2: Rationale

1) Inadequacy or absence of sound KYC principles can subject banks and financial institutions to serious customer and counter-party risks especially reputational, operational, legal and concentration risks. Any one or a combination of these risks can result into significant financial loss to banks or financial institutions (eg through the withdrawal of funds by depositors, termination of inter-bank or correspondent banking facilities) which may affect their safety and soundness.

2) Banks and financial institutions can be involved in a financial crime as a victim, perpetrator or vehicle. Financial institutions can be subject to fraud (eg cheque fraud) perpetrated by customers in collusion with insiders. They can also be used as a conduit or instrumentality to keep or transfer proceeds of crime. Institutions must therefore be familiar with three stages of money laundering: placement, layering and integration.

3) Occurrence of financial crime may lead to loss of depositors' confidence in the integrity of the institution. Trust underpins the existence of financial

systems and the effective functioning of a financial system relies heavily on the expectation that high professional, legal and ethical standards are observed and enforced. A reputation for integrity-soundness, honesty, adherence to standards and ethics- is one of the most valued assets of a financial institution and the entire system as a whole.

4) Sound KYC policies, practices and procedures with respect to customer identification and on-going monitoring of accounts and transactions, should therefore constitute an essential part of sound risk management of each bank or financial institution.

PART III: EFFECTS OF ABSENCE OF (OR INADEQUATE) KYC PRINCIPLES

Sec. 1: Operational Risks

1) Operational risk is defined as the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events.

2) Most operational risk in KYC context relates to weaknesses in the implementation of an institution's programmes, ineffective internal procedures and failure to practice due diligence which may directly result into financial loss.

Sec. 2: Reputational Risks

1) Reputational risk is defined as the potential that adverse publicity regarding a bank or financial institution's business practices, whether accurate or not, will cause loss of confidence in the integrity of the institution.

2) A bank or financial institution can easily become a victim or vehicle for illegal activities perpetrated by its customers or employees. Incidences of frauds may indicate that the concerned institution is not managed with integrity and skills expected of a banking organization. Public perception that the institution is not able to manage its operational risks effectively can damage its reputation.

3) Public confidence in banks and financial institutions can also be undermined, and the reputation of the bank damaged, as a result of association with drug traffickers and other criminals.

4) Loss of confidence may adversely affect the business of a bank or financial institution and the integrity of the entire banking system. In view of this, every institution needs to protect itself by means of continuous vigilance through an effective KYC programme.

Sec. 3 Legal Risks

1) Legal risk is the possibility that lawsuits, adverse judgments or contracts that turn out to be unenforceable can disrupt or adversely affect the operations or condition of a bank or financial institution.

2) A bank or financial institution may be subject to lawsuits resulting from the failure to practice due diligence on its customers. The institution may be unable to protect itself effectively from such legal rights if they do not engage in due diligence in identifying their customers and understanding their business.

3) An institution's exposure may lead to reputational and financial losses which may eventually affect its own integrity as well as that of the entire system.

Sec. 4 Concentration Risk

1) Concentration risk applies both to the asset and liability sides of the balance sheet. Restrictions are normally imposed to prevent an institution's exposure to single borrowers or group of related borrowers from exceeding prescribed limits.

2) If the bank or financial institution does not precisely know who its customers are and their relationship with other customers, it is not possible for a bank to measure the concentration risk. This is particularly relevant to related counter parties and connected lending.

3) On the liabilities side, deposit concentration may also affect funding, particularly the risk of early and sudden withdrawal of funds by large depositors. A bank or financial institution should understand the characteristics of their customers/depositors, including not only their identities but also the extent to which their actions may be linked with those of other depositors.

4) To effectively manage risks arising from such accounts, a bank or financial institution should be able to aggregate and maintain balances and activity in these accounts.

PART IV ELEMENTS OF KYC STANDARDS

In view of potential loss arising from exposure to the foregoing risks, every bank or financial institution should have effective KYC practices as part of its risk management and internal control systems.

Sec. 1: Customer Acceptance Policy

1) The board of every bank or financial institution shall be responsible for the establishment of customer acceptance policies and procedures including a description of the type of customers that are unacceptable to bank.

2) In preparing such policies, factors such as customer's background, country of origin, public or high profile position, business activities or other risk indicators should be considered.

3) Banks are encouraged to develop graduated customer acceptance policies and procedures that require more extensive due diligence for high risk customers. Decisions to enter into business relationship with high risk customers, such as politically exposed persons should be taken exclusively at senior management level.

4) The policies and written procedures shall be communicated to all relevant personnel and that on-going training program shall be put in place to ensure that bank staff are adequately trained in KYC procedures to facilitate the recognition and reporting of suspicious transactions .

5) Every bank or financial institution shall appoint a senior officer with explicit responsibility for ensuring that the bank's policies and procedures are implemented effectively.

Sec. 2: Customer Identification

1) Every bank or financial institution shall establish a systematic procedure for verifying the identity of new customers and should never enter into a business relationship until identity of such a customer has been satisfactorily established. The institution should document and enforce policies for identification of customers and those acting on their behalf.

2) The prospective customers should be identified on the basis of a reliable and independent source document such as a birth certificate, passport, driving licence and a letter of recommendation from an existing customer or employer and such an identity should be recorded. The identity of occasional customers should also be verified and recorded when performing transactions over a specified threshold. Identification of customers should be renewed in the course of their business relationship when doubts appear as to their true identity.

3) If the prospective customer is a legal entity, a bank or financial institution should adequately verify its legal existence and structure, including information concerning (a) the customer's legal name, legal form, postal and physical addresses, directors, owners (b) provisions regulating the power to bind the entity. The identity of the person purporting to act on behalf of the entity and his/her authority to do so should also be verified.

4) A bank or financial institution should never open an account or conduct on-going business with a customer who insists on anonymity or bearer status or gives a fictitious name. Confidential numbered accounts should be subject to exactly the same KYC procedures as all other customers. Numbered accounts should only be permitted if the financial institution has properly identified the customer in accordance with the set criteria, and the customer identification documents are available to compliance officers and bank supervisors.

5) If a bank or financial institution is aware that it lacks sufficient information about an existing high risk customer, it should take steps to ensure that all relevant information is obtained as quickly as possible. In any case, banks should undertake regular review of its customer base to establish that it has up-to-date information and a proper understanding of its account holders' identity and of their business.

6) Where customers are acting on behalf of another person as trustee, nominee or professional intermediary, a bank or financial institution should receive satisfactory evidence of the identity of the intermediary

and of the person on whose behalf they are acting as well as the nature of the trust or other arrangements in place.

7) Relying on due diligence conducted by an introducer, however reputable, does not in any way remove the ultimate responsibility of the recipient bank or financial institution to know its customer and business.

Sec. 3: On-going Monitoring of Accounts and Transactions

1) A bank or financial institution shall take reasonable steps to conduct on going scrutiny of any transaction undertaken throughout the course of the business relationship with a customer to ensure that the transaction being conducted is consistent with the bank's or financial institution's knowledge of the customer, the customer's business and risk profile, including where necessary, sources and applications of funds.

2) A bank or financial institution shall ensure that it has adequate management information systems to provide managers and compliance officers with timely information needed to identify, analyse and effectively monitor high risk customer accounts.

3) A bank or financial institution shall pay particular attention to all complex, unusually large transactions and all unusual patterns of transactions that have no apparent or visible economic or lawful purposes, and shall examine as far as possible, the background and purpose of such transactions and set forth findings in writing.

4) A bank or financial institution shall have systems in place to detect unusual or suspicious patterns of activity. Certain patterns of transactions should alert the banks and financial institutions to the possibility that the customer is conducting undesirable activities. They may include transactions that do not make economic or commercial sense, or that involve large amounts of cash deposits that are not consistent with the usual 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.

5) A bank or financial institution shall develop a clear policy and internal guidelines, procedures and controls and remain especially vigilant regarding business transactions with politically exposed people (PEP) or with persons and companies that are clearly related or associated with them.

Sec. 4: Reporting of Suspicious Transactions to the Reserve Bank

1) If a bank or financial institution has reasonable grounds to suspect or suspects that a transaction or an attempted transaction, or information that it has concerning any transaction or attempted transaction either stems from a criminal activity or is linked or related to, or is to be used to finance terrorism, it shall report promptly to the Reserve Bank of Malawi indicating the amount involved, the nature of the transaction, the person or persons involved and the date of the transaction etc.

2) Save for purposes of obtaining information necessary to complete a

Suspicious Transaction Report (STR), banks and financial institutions shall not be responsible for conducting follow-up investigations of suspicious transactions.

3) No director, manager, officer or employee of a bank or financial institution shall disclose to any person, other than the Reserve Bank of Malawi or when required to do so in court, that a particular institution has formed a suspicion in relation to a transaction or that a report to the Reserve Bank has been, or may be, made under this Directive.

4) Neither a reporting institution nor its director, manager, officer or employee shall be subject to a claim, suit, liability or other proceedings in respect of anything done with due diligence and in good faith, in pursuance, execution, or exercise of powers and obligations conferred on that institution or individual under this Directive.

Sec. 5: Record Keeping

1) A bank or financial institution shall maintain all necessary records concerning customer transactions and accounts for at least 7 years, following completion of the transaction, regardless of whether the account or business relationship is terminated.

2) A bank or financial institution shall maintain records on customer identity account files and business correspondence and all relevant records for at least seven years following the termination of a business relationship or closure of an account.

3) Transaction records should be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal behaviour. A bank or financial institution shall ensure that customer and transaction documents and information are available to supervisory authorities and any other relevant competent authorities without breaching customer confidentiality.

4) Banks and financial institutions should establish an effective means of testing for general compliance with policies, procedures and controls relating to KYC.

Sec 6 Compliance

1) To ensure compliance, a bank or financial institution shall:

a) Provide for and document a system of internal controls;
b) Provide for and document independent testing for compliance to be conducted by bank personnel or by an outside party on a regular basis;
c) Designate an individual or individuals responsible for coordinating and monitoring day-to-day compliance; and
d) Provide for and document training to all appropriate personnel, on at least an annual basis, of the content and required procedures of the KYC programme.

PART V – COOPERATION AMONGST BANKS AND FINANCIAL INSTITUTIONS

Sec 1: 1) **Exchange of Information**

Banks and financial institutions shall cooperate spontaneously or upon request, with each other with respect to investigation and verification of identity of a prospective or an existing customer in accordance with the requirements of this Directive.

PART VI - INSPECTIONS BY THE RESERVE BANK

Sec. 1: **Inspections to Determine Compliance with this Directive**

1) Bank supervisors shall conduct inspections of the head office and all branches of every bank or financial institution to verify establishment and implementation KYC policies and procedures on a continuous basis.

2) The supervisory process shall include, but not restricted to, a review of policies and procedures, customer files and the sampling of accounts.

PART VII: REMEDIAL MEASURES AND ADMINISTRATIVE SANCTIONS

Sec. 1: **Remedial Measures**

If the Reserve Bank determines that a bank or financial institution is not in compliance with this Directive, then:

1) The Reserve Bank shall impose civil money penalties on the non-compliant institution amounting to Malawi Kwacha equivalent of US10,000 or 1% of its latest core capital whichever is higher.

2) The Reserve Bank may impose remedial measures as specified under Sections 31 of the Banking Act.

Sec. 2: **Administrative Sanctions** –

In addition to the remedial measures available to it as given in Section 1 above, the Reserve Bank may impose any or all of the following administrative sanctions with regard to a bank or financial institution that is not in compliance with this directive:

1) Suspension of the establishment of new branches and/or expansion into new banking or financial activities;

2) Suspension of access to credit facilities of the Reserve Bank;

3) Suspension of the opening of letters of credit;

4) Suspension of the acceptance of new deposits;

PART VIII: EFFECTIVE DATE

This Directive shall come into force with effect from 1st January 2005. However, all banks and financial institutions are urged to review and regularise all existing

accounts in accordance with the requirements of this Directive within a period of six months.

Questions relating to this directive should be addressed to the Director, Bank Supervision Department of the Reserve Bank of Malawi.

Dr Ellias E. Ngalande
GOVERNOR