PUBLIC INSTRUCTION № 02/2004
ON THE PREVENTION OF MONEY LAUNDERING, CUSTOMER IDENTIFICATION AND RECORD-KEEPING

The Governing Board

Pursuant to:

1. Section 17.b) of UNTAET Regulation № 2001/30 giving BPA the authority to issue rules, instructions, and guidelines;
2. Section 21 of UNTAET Regulation № 2000/8 concerning prevention of money laundering;
3. Section 23.1 of UNTAET Regulation № 2000/8 concerning general prudential principles;
4. Section 47.1 of UNTAET Regulation № 2000/8 concerning the publication of BPA Instructions in the Official Gazette;
5. Section 36 of UNTAET Regulation № 2000/8 concerning infractions, penalties and remedial measures;
6. Section 165 of the Constitution of the Democratic Republic of Timor-Leste concerning the continued applicability of laws in force at the date the adoption of the Constitution.

Taking into account that:

1. a bank or the banking system may be exposed to reputational, operational, legal and other risks related with money laundering activities;
2. the involvement of banking institutions in money laundering is likely to seriously undermine their reputation and undermine the public's confidence in them and in the banking system.
3. the effective knowledge and understanding by banks of their customers and the business that they conduct with or through the banking institution is essential in preventing the banking system from being used for money laundering;

For the purpose of:

1. reducing the risk of the banking system becoming a vehicle for/or a victim of financial crime and suffering consequential damage, and
2. protecting the reputation and integrity of the banking system.

HEREBY RESOLVES TO APPROVE THE FOLLOWING

PUBLIC INSTRUCTION № 02/2004
ON THE PREVENTION OF MONEY LAUNDERING, CUSTOMER IDENTIFICATION AND RECORD-KEEPING

Section 1
Applicability

This Public Instruction shall apply to all banks and to all branches of foreign banks licensed to operate in Timor-Leste.

Section 2
Definitions

In this present Public Instruction:

"Bank" means a person engaged in the business of accepting deposits from the public in Timor-Leste and using such funds, either in whole or in part, to make extensions of credit or investments for the account of and at the risk of the person carrying on the business;

"BPA" means Banking and Payments Authority of Timor-Leste.

"Compliance Officer" means an officer who is responsible for ensuring that a bank complies with its obligations in accordance with the present Public Instruction.

"Financial documents' means a security, bank draft or other written commitment by a bank to pay money, which can be transferred by delivery or endorsement.

"Numbered accounts" means accounts in which the name of the beneficial owner is known to the bank but is substituted by an account number or code name in some documentation.

"Politically Exposed Persons" (PEPs) means individuals, resident and non-resident, 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 as well as persons or companies clearly related to them (i.e. families, close associates, etc).

Section 3
Know Your Customer ("KYC") Policy and Procedures

1. The board of directors of each bank shall establish policies with regard to KYC which shall include reference to the following:
   (1) Customer acceptance;
   (2) Definitions of types of customer likely to represent high risk;
   (3) Different rules for different types of customers.

2. In formulating the policy, factors such as the customer's background, his/her public status, accounts related to the customer's account and the extent of his/her business activities shall be taken into consideration.

3. Management of the bank shall determine and implement KYC procedures in accordance with the policy set by the board of directors and with its risk assessment, which shall ensure ethical and professional standards that will prevent the bank from being exploited, intentionally or unintentionally, by persons engaged in criminal activities wishing to conceal or disguise the illicit origin of the property or of any person assisting with such activities.

4. The procedures shall cover, among others, the subjects in this Public Instruction, the reporting system and the staff authorized to handle the reports, the types of record that shall be retained relating to customer identification and to specific transactions, and the period of their retention.

5. The compliance officer shall be appointed and shall submit a quarterly assessment report to the management of the bank regarding the implementation of its KYC policies and procedures, taking into account requirements derived from applicable laws, regulations and provisions. Such assessment report shall be made available for BPA's examiners during onsite examination.

6. Banks shall incorporate the following basic KYC principles in the risk-management and internal control systems:

   (1). Customer acceptance;

   (2). Customer identification;

   (3). On-going monitoring and control of high-risk accounts.

Section 4
Customer Acceptance Policy

1. Banks shall develop customer acceptance policies and procedures whose objective shall be to identify the types of customer that are likely to pose a higher than average risk of money laundering. A more extensive customer due diligence process should be adopted for higher risk customers. There shall also be clear internal guidelines on which level of management is able to approve a business relationship with such customers.

2. In determining the risk profile of a particular customer or type of customer, banks shall take into account at least the following factors:

   (a) the origin of the customer (e.g. place of birth, residency), the place where the customer's business is established, the location of the counterparties with whom the customer conducts transactions and does business, and whether the customer is otherwise connected with certain jurisdictions such as Non-Cooperative Countries and Territories (NCCTs) designated by the Financial Action Task Force (FATF), or those known to the bank to lack proper standards in the prevention of money laundering or customer due diligence process;

(b) the background or profile of the customer such as being, or linked to, a politically exposed person or otherwise being an individual with high net worth whose source of funds to be credited to an account (both initially and thereafter) is unclear;

(c) nature of the customer's business, which may be particularly susceptible to money laundering risk, such as money changers, lottery operators or casinos that handle large amounts of cash;

(d) for a corporate customer, an unduly complex structure of ownership for no apparent commercial reason; and

(e) any other information that may suggest that the customer is of higher risk (e.g. knowledge that the customer has been refused a banking relationship by another bank).

3. Following the initial acceptance of the customer, banks shall monitor the pattern of account activity and if the pattern does not conform to the bank's understanding of the customer, the bank shall review the customer's status, and if appropriate reclassify the customer as higher risk.

Section 5
Customer Identification

1. Banks are prohibited from dealing with unknown customers. Banks shall cease to deal with customers who refuse to provide the details required to enable compliance with this Public Instruction.

2. The customer identification process shall comprise the following:

   (a). identify the direct customer, i.e. know who the individual or legal entity is;

   (b). verify the customer's identity using reliable, independent source documents, data or information;

   (c). identify beneficial ownership and control, i.e. determine which individual(s) ultimately own(s) or control(s) the direct customer, and/or the person(s) on whose behalf a transaction is being conducted;

   (d). verify the identity of the beneficial owner of the customer and/or the person on whose behalf a transaction is being conducted, corroborating the information provided in relation to (c); and

   (e). conduct on-going due diligence and scrutiny i.e. perform on-going scrutiny of the transactions and account throughout the course of the business relationship to ensure that the transactions being conducted are consistent with the bank's expectation and knowledge of the customer, its business and risk profile, including, where necessary, identifying the source of funds.

3. The identity of an individual includes the individual's name (including former or other name), residential address (and permanent address if different), date of birth and

nationality. To facilitate on-going due diligence and scrutiny, information on the individual's occupation or business should also be obtained.

4. Objection of the customer, without good reason, to provide the information requested and to cooperate with the bank's customer due diligence process shall itself be a factor that should trigger suspicion.

5. Where a bank allows confidential numbered accounts, the same customer due diligence process should apply even if this is conducted by nominated staff. The identity of the account holder shall be known to a sufficient number of staff to operate proper due diligence. Such accounts should in no circumstances be used to hide the customer identity from the bank's compliance function or from the BPA.

6. Banks shall not in general establish a business relationship with a new customer until the due diligence process is satisfactorily completed. However, it may be acceptable to allow an account to be opened pending completion of the verification of identity provided that the necessary evidence of identity is promptly obtained. In such a case banks shall not allow funds to be paid out of the account to a third party before the identity of the customer is satisfactorily verified.

7. If an account has been opened but the process of verification of identity cannot be successfully completed, the bank shall close the account and return any funds to the source from which they were received.

8. After a business relationship has been established, banks shall undertake regular reviews of the existing records relating to the customer to ensure that they remain up-to-date and relevant.

9. Banks shall not open an account for a customer who is acting on behalf of a third party who does not provide the information required regarding the third party.

10. A bank that has cause to believe that an applicant has been refused banking services by another bank for reasons related to the prohibition on money laundering shall apply enhanced diligence procedures in opening an account for that customer.

Section 6
Politically Exposed Persons

The following procedures shall be adopted when dealing with PEPs:

(1) On opening an account for a new customer, banks shall check whether the customer is a public figure.

(2) Banks shall take steps to discover the source of funds expected to be deposited in the account, before opening an account for a PEP.

(3) The decision to open an account for a PEP shall be taken by a senior manager.

(4) The account of a PEP shall be considered a high-risk customer account.

Section 7
Updating Customers' Particulars

If a customer advises the bank of a change of mailing address:

(1) Banks shall update the address in all that customer's accounts with the same account number for which the customer originally gave that mailing address, unless instructed otherwise.

(2) Banks shall draw the attention of the customer to the need to update the address in his other accounts, if any.

Section 8
Transfer of Money

1. Every document of a cash transfer or of a transfer of a financial document shall include the name and bank account number of the payee, if any.

2. In transferring money abroad by electronic means (e.g. SWIFT), banks shall indicate the name and account number of the customer making the transfer.

3. A bank shall decline to transfer money to or from high risk customer accounts, or to or from other customer accounts, where it has cause to believe that the transaction may be undertaken for the purpose of transferring, concealing or disguising the illicit origin of money or assisting any person who is involved in such activity, or otherwise contravenes the principles established in this Public Instruction.

Section 9
Retention of Identification Documents

1. Banks shall establish procedures for the retention of information essential for authenticating customers' identity and their type of business, relating to the source of the information, the period for which it should be retained, the type of customer (individual, company, etc.), and the expected extent of activity in the account. The information shall be retained in a manner which will make it readily available and enable efficient retrieval.

2. (a) Banks shall undertake reviews to ascertain the existence of adequate and updated information.

   (b) The reviews shall take place at times and on occasions determined by the bank in its procedures, such as when a significant transaction is about to take place, or when the requirements relating to customer documentation change, or when the way the account is managed alters significantly.

   (c) If bank discovers that certain significant information about a customer is lacking, it shall take steps to ensure that it obtains the missing information as soon as possible.

Section 10
On-Going Monitoring of Accounts and Transactions

1. Banks shall operate a system to detect unusual activities in all its customers' accounts. This can be done by setting limits for certain categories of accounts. Unusual activities may include transactions that appear to lack economic or commercial sense, or that involve large sums of money, particularly large cash deposits not consistent with the expected activity in the account.

2. Banks shall set detailed procedures setting out the channel of communications regarding unusual transactions which the bank has reasonable grounds to suspect of being associated with money laundering. The procedures should incorporate full documentation of the decision making process from the first detection of the unusual transaction to the formulation of a decision on whether to report to the competent authority.

3. Banks shall verify the identities of the parties to a transaction which is likely to constitute a significant risk to the bank.

Section 11
High-Risk Customer Accounts

1. Banks shall include in their procedures rules for defining high risk customer accounts with regard to the prohibition on money laundering. In formulating these rules banks shall take into consideration the type of business (e.g., a cash-intensive business), the location of the customer's activity (e.g., in countries categorized by the Financial Action Task Force on Money Laundering (FATF) as Non-Cooperative Countries and Territories), the types of services required by the customer (e.g., electronic transfers of large sums), and the type of customer (e.g., a prominent public figure from abroad, an entity with a complex ownership structure) and politically exposed persons.

2. Banks shall operate appropriate intensified systems for monitoring these customer's accounts and shall follow up on high-risk accounts by setting key indicators for such accounts, taking note of the background of the customer, the country of origin of the funds, and the type of transactions involved.

3. Banks shall operate an adequate information system to provide officers responsible with timely information needed to analyse and effectively monitor high-risk customer accounts. Such reports shall include unusual transactions performed through the customer's account, information on the relationship between banks and that customer over time, and also information on missing account-opening documentation.

4. Significant transactions which customers categorized as high risk wish to perform shall require the approval of a senior manager.

Section 12
Training

Banks shall provide training on customer due diligence and KYC policy and procedures, distinguishing between new staff, management staff, branch staff, staff who deal with the acceptance of new customers, and those engaged in compliance, and shall make all employees aware of the procedures it has set.

Section 13
Reporting of Suspicious Transactions

1. Banks shall immediately report to BPA any customer activity that may adversely affect the stability or reputation of the bank.
2. Banks shall report to the BPA the names of customers whose applications for opening an account with bank have been refused.
3. Banks shall immediately report to the BPA any law enforcement inquiry relevant to money laundering being conducted in the bank or a company under its control.
4. Banks shall immediately report to the BPA any transaction declined by the bank pursuant to this Public Instruction.

Section 14
Infractions, Penalties and Remedial Measures

1. Banks, their principal shareholders and/or any of their administrators shall be subject to penalties where the BPA determines that the provisions of this Public Instruction have been violated.
2. The BPA may impose penalties of between $ 500 and $ 5,000 per day where an account is accepted in contravention of the KYC principles, maintained for a customer where no proper identification is kept on file, is not regularly reviewed, or otherwise maintained in contravention of the provisions of this Public Instruction.
3. The BPA may impose penalties of up to $ 5,000 per transaction for transactions made in violation of this Public Instruction, or for suspicious transactions not reported to the BPA.
4. The powers set out in this Section shall not restrict the general powers of the BPA to issue written warnings, suspend or dismiss administrators, to revoke the license of banks, or other powers conferred by legislation.

Section 15
Transitional Provisions

1. Banks shall immediately review their customer data base to ensure that it has complete information to comply with this Public Instruction.
2. Where such information is insufficient, banks shall update the customer data base within six months effective from the date this Public Instruction enters into force.

Section 16
Publication

For the information of the public, this Public Instruction shall be published in the Official Gazette.

Section 17
Entry Into Force

This Public Instruction shall enter into force on the date of its publication.

Signed at Dili, this 7th day of May, 2004

Luis Quintaneiro
Chairman