B 7-08-089 Pro Kor

Unofficial Translation

PRAKAS
ON
ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM

The Governor of the National Bank of Cambodia

- With reference to the Constitution of the Kingdom of Cambodia;

- With reference to the Royal Kram NS/RKM/0196/27 of January 26. 1996 promulgating the *Law on the Organization and Conduct of the National Bank of Cambodia*;

- With reference to the Royal Kram NS/RKM/1199/13 of November 18. 1999 promulgating the *Law on Banking and Financial Institutions*;

- With reference to Royal Kram NS/RKM/0607/014 of June 24. 2007 promulgating the *Law on Anti-Money Laundering and Combating the Financing of Terrorism*;

- With reference to the Royal Decree NS/ RKT/0508/526 of May 13, 2008 on the appointment of His Excellency Chea Chanto as Governor of the National Bank of Cambodia, which is equivalent to Senior Minister.

- Pursuant to the request of the General Direction

- Pursuant to the spirit of the meeting of the senior management of the National Bank of Cambodia dated May 27, 2008

DECIDES

Article 1 - Scope

For the purposes of the present Prakas the term ‘banks and financial institutions” shall apply to the following institutions and professions, when they are regulated by the National Bank of Cambodia and referred to as “reporting entities” in the *Law on Anti-Money Laundering and Combating the Financing of Terrorism*:

a) banks, including branches of foreign banks;

b) micro-finance institutions;

c) credit cooperatives;

d) leasing companies;

e) exchange offices/moneychangers;

f) money remittance services;

g) dealers in precious metals, stones and gems;

h) Any other institution or profession that is designated by the Financial Intelligence Unit to fall within the scope of the *Law on Anti-Money Laundering and Combating the Financing of Terrorism* and is supervised by the National Bank of Cambodia.

Article 2 – Customer Acceptance Policy

Banks and financial institutions should develop customer acceptance policies and procedures and should have reasonable measures, including risk profile, in their internal policy and procedures to address different risks posed by each type of customer or by each individual customer.

Article 3 – Risk Profiling

3.1 In creating the risk profile of a type of customer or an individual customer, banks and financial institutions should at least take into consideration the following factors:

- ❖ the origin of the customer and location of business;
- ❖ background and personal particulars of the customer
- ❖ nature of the customer's business;
- ❖ structure of ownership for a corporate customer; and
- ❖ any other information indicating the customer is of higher risk

3.2 Following the initial acceptance of the customer, banks and financial institutions should continuously monitor the customer's account activity pattern to ensure it is in line with the customer profile. Unjustified and unreasonable differences should cause banks and financial institutions to reassess the customer as higher risk.

Article 4 – Prohibition of Anonymous Account and Accounts in Fictitious Names

Banks and financial institutions should ensure that an account is opened and maintained in the name of the account holder at all times. In addition, banks and financial institutions should establish customer identity as outlined in articles 6 and 7 of the present Prakas and ensure that no customer is allowed to open or operate an anonymous account or an account in a fictitious, false or incorrect name.

Article 5 – Customer Due Diligence

5.1 Banks and financial institutions must conduct customer due diligence and obtain satisfactory evidence and properly establish in its records the identity and legal

existence of persons applying to do business with them. Such evidence must be substantiated by reliable documents.

5.2 The customer due diligence should be conducted, when:

- establishing business relationship with the customer such as opening an account, granting a safe deposit facility or engaging in any other business dealings;
- carrying out an occasional or one off transaction, that involves a sum in excess of USD 10,000 (or 40 million Riels or foreign currency equivalent) or wire-transfer in excess of USD 1,000 (or 4 million Riels or foreign currency equivalent).
- banks and financial institutions have any suspicion of money laundering or financing of terrorism; or
- banks and financial institutions have any doubts about the veracity or adequacy of previously obtained information.

5.3 The customer due diligence undertaken by banks and financial institutions should at least comprise the following:

- identify the customer and verify the identity of the customer using reliable, independent source documents, data or information referred to in articles 6 or 7;
- determine if the customer conducting business is acting on behalf of another person or beneficial owner;
- understanding the beneficial ownership and control structure of the customer. Beneficial owner is defined in article 8;
- obtain information on the purpose and intended nature of the business relationship; and
- conduct on-going due diligence and scrutiny, to ensure the information provided is updated and relevant and ensure that the transactions being conducted are consistent with the bank's or financial institution's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.

5.4 Unwillingness of the customer to provide the information requested and to cooperate with banks and financial institutions' customer due diligence process may itself be a factor of suspicion.

5.5 Banks and financial institutions should not open the account, commence business relations or perform transaction, or in the case of existing business relations with customers, it should terminate such business relations if the customer fails to comply with the customer due diligence requirements. Such situation warrants a suspicious transaction report to be submitted to the Financial Intelligence Unit.

Article 6 - Individual Customers

6.1 In establishing a business relationship with an individual customer, banks and financial institutions should obtain from the individual customer at least the full name, date of birth, identity card/passport number/identity document reference number, occupation/business, address and nationality.

6.2 Banks and financial institutions should require the individual to furnish the original and make copies of one or more of the following documents:

- National identity card;
- Passport; or
- Identity documents preferably bearing a photograph of the customer, issued by an official authority.

Article 7 - Corporate Customers

7.1 In establishing a business relationship with a corporate customer, banks and financial institutions should require the company/business to furnish the original and make copies of at least the following documents:

- Memorandum/Article/Certificate of Incorporation/Partnership
- Identification document of Directors/Shareholders/Partners
- Board of Directors'/Directors' Resolution
- Authorisation for any person to represent the company/business
- Authorisation or permit to conduct business

7.2 In addition, banks and financial institutions should conduct a basic search or enquiry on the background of such company/business to ensure that it has not been, or is not in the process of being, dissolved or wound-up.

7.3 The identity of all account signatories shall be verified according to customer due diligence for individual customers. When signatories change, care should be taken to ensure that the identity of all current signatories has been verified.

7.4 To verify the information provided, banks and financial institutions should check with the Registry of Companies/Businesses on the authenticity of the information provided on the identity of the company/business and its directors, owners, shareholders and office bearers.

7.5 Where the customer or the owner of the controlling interest is a public company that is subject to regulatory disclosure requirements i.e. a public company listed on a recognised stock exchange, it is not necessary to seek to identify and verify the identity of the shareholders of that public company.

7.6 Banks and financial institutions should also understand the ownership and control structure of corporate customers and determine the source of funds of the company/business. This will assist banks and financial institutions in ascertaining any suspicion concerning the changes to the ownership or control structure and in developing the customer profile and expected activity through the company/business account.

Article 8 - Beneficial Owner

Banks and financial institutions should conduct customer due diligence as stringent as the one imposed on individual customer when they suspect a transaction is conducted on behalf of a beneficial owner and not the customer who is conducting such transaction. Beneficial owner is the natural person(s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being

conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement.

Article 9 – Non-Government Organization and Foundation

9.1 Banks and financial institutions should require a Non-Government Organization or foundation establishing business relationship to furnish the constitution documents or other similar documents to ensure that it is properly constituted and registered.

9.2 The identity of all account signatories shall be verified according to customer due diligence for individual customers. When signatories change, care should be taken to ensure that the identity of all current signatories has been verified.

9.3 Banks and financial institutions should take steps to understand who is in control and makes decisions regarding the Non-Government Organization/foundation, and the use of the funds.

Article 10 - Trust and Nominee Accounts

10.1 Banks and financial institutions need to establish whether the customer is acting on behalf of another person as trustee, nominee or agent.

10.2 Banks and financial institutions should take reasonable measures to understand the ownership and control structures and the relationship among the relevant parties in handling a trust or nominee account and obtain evidence of the identity of the settler, trustee, nominee, authorised signatories, persons exercising effective control and the beneficiaries.

10.3 Banks and financial institutions should ensure customer due diligence requirements are completed for beneficial owners, when the trust or nominee account is established.

10.4 Banks and financial institutions require a written assurance from the trust or nominee that evidence of the identity of the beneficiaries has been obtained, recorded and retained, and that the trust or nominee is satisfied regarding the source of funds. In addition, identification information must be immediately available to banks and financial institutions upon request.

Article 11 - Client Accounts

Banks and financial institutions should satisfy themselves about transactions passing through lawyers and accountants clients' accounts that give cause for concern, and should report those transactions to Financial Intelligence Unit, if any suspicion is aroused.

Article 12 - Shell Companies

Banks and financial institutions should not open an account for or conduct business with a shell company, which do not conduct any commercial activities or have any form of commercial presence in the country but are legal entities through

which financial transactions may be conducted.

Article 13 - Reliance on Intermediaries or Other third Parties for CDD or Introduced Business

13.1 Banks and financial institutions should be wary and ensure that they do not fall complacent and completely rely on the customer due diligence conducted by the intermediaries or other third parties they use. The ultimate responsibility of customer due diligence always remains with banks and financial institutions.

13.2 Banks and financial institutions must be satisfied that the introducing intermediary:

- ❖ has carried out customer due diligence by identifying the customer and verify that identity using reliable, independent source documents, data or information;
- ❖ has identified the beneficial owner and in respect of corporate customers understands the ownership and control structure of the customer;
- ❖ understands the purpose and nature of the business relationship;
- ❖ has put in place a system to provide the bank or financial institution with access to the identification documents, data or information upon request and without delay;
- ❖ allows periodic review by banks and financial institutions to verify the due diligence undertaken; and
- ❖ is properly regulated and supervised for AML/CFT purposes by the respective authority.

Article 14 – Non Face-to-Face Customers

14.1 Banks and financial institutions should pay special attention in establishing and conducting non-face-to-face business relationships and undertake customer due diligence through face-to-face interaction, or through an intermediary as required by article 13 of the present Prakas, prior to establishing such business relationships with their customers.

14.2 Banks and financial institutions are also required to implement monitoring and reporting mechanisms to identify potential money laundering and financing of terrorism activities.

Article 15 - Correspondent Banking

15.1 Banks and financial institutions should take the necessary measure to ensure that they are not exposed to the threat of money laundering and financing of terrorism through correspondent accounts they have with other banks and financial institutions.

15.2 Banks and financial institutions entering a correspondent relationship should gather and assess at least the following information on the correspondent banks and financial institutions;

- ❖ board of director and management;
- ❖ business activities and products;
- ❖ subjected legislations, regulation and supervision;
- ❖ AML/CFT measures and controls; and

- ❖ annual reports.

15.3 Banks and financial institutions should establish or continue a correspondent banking relationship with the correspondent banks and financial institutions only if it is satisfied with the assessment of the information gathered.

15.4 Banks and financial institutions should also document the responsibilities of the respective parties in relation to the correspondent banking relationship.

15.5 The decision and approval to establish or continue a correspondent banking relationship should be made at the Senior Management level.

15.6 Banks and financial institutions, should ensure that such correspondent banking relationship do not include correspondent banks and financial institutions that have no physical presence and which is unaffiliated with a regulated financial group.

15.7 Banks and financial institutions should exercise enhanced due diligence with respect to correspondent banks and financial institutions which allow direct use of the correspondent account by their customers to transact business on their own behalf such as payable–through accounts. Banks and financial institutions should implement customer due diligence for such customers as required for intermediaries introducing business.

15.8 Banks and financial institutions should pay special attention to correspondent banking relationship with correspondent banks and financial institutions from countries which have insufficiently implemented the internationally accepted AML/CFT measures. Enhanced due diligence is needed to assess the money laundering and financing of terrorism risks.

Article 16 - Remittance / Wire Transfer

16.1 Banks and financial institutions conducting or participating in an outgoing remittance/wire transfer transaction should include with it the necessary originator's name, address, account number, identification number or customer reference number and the details of the transaction.

16.2 Banks and financial institutions facilitating or acting as intermediary to a remittance/wire transfer transaction should ensure such originators information is still retained with remittance/wire transfer message.

16.3 Banks and financial institutions receiving a remittance/wire transfer message with incomplete originators information should conduct enhanced due diligence and may consider it as a factor of suspicion.

16.4 It is not necessary to include all the above information in the message accompanying a remittance/wire transfer transaction of less than USD 1,000/Riel 4 Million or its equivalent in any other currencies.

16.5 Banks and financial institutions should pay attention to wire transfers by higher risk customers and consider such factors as the name of the beneficiary, the destination and amount of the remittance/wire transfer. The customer should be

asked to provide further explanation of the nature of any remittance/wire transfer which is inconsistent with the customer's usual business/activity.

Article 17 - Politically Exposed Persons (PEPs)

17.1 Banks and financial institutions should check current and new customers to determine whether they are Politically Exposed Persons, as defined in article 3 of the Law on Anti-Money Laundering and Combating the Financing of Terrorism, as part of the customer due diligence process. Banks and financial institutions should gather sufficient information from the said customer and research further data or information to determine the level of AML/CFT risk.

17.2 Once a PEP is identified, banks and financial institutions should take reasonable measures to establish the source of wealth and funds of such persons.

17.3 The decisions to enter into or continue business relationships with these PEPs should be made by the senior management of banks and financial institutions.

17.4 Banks and financial institutions should develop a risk profile of each PEP based on information collected from the customer and obtained through independent research and understand the full nature of the business relationship and transaction activity. There should be on-going monitoring of the relationship and activity against the risk profile and any concerns arising from the monitoring process should be reported to senior management and, if appropriate, also reported to the Financial Intelligence Unit.

Article 18 - Private Banking

18.1 Private banking businesses are provided to high net worth customers and very important people and its exclusive, confidential and private nature gives rise to the possibility of abuse by money launderers and financiers of terrorism.

18.2 Banks and financial institutions should give special attention to customers of private banking business. The identification and verification procedures should be more stringent than normal identification procedures. In particular, additional verification measures should be implemented regarding identification of customer, nature of business and source of funds.

18.3 All new and existing customers within the private banking service must undergo approval by senior management other than the manager of the private banking relationship who processes and recommends the application.

18.4 The compliance officers and auditors must be allowed to audit and review the transactions of private banking customers.

Article 19 - Moneychangers

19.1 Banks and financial institutions must pay special attention to and ensure that the moneychangers who maintain accounts with them are licensed and only conduct legitimate currency exchange transactions. Banks and financial institutions should ensure that the nature and volume of transactions in the moneychangers account reflect the nature of their business.

19.2 If banks and financial institutions identify any discrepancies in the activities of the moneychangers account, they should submit a suspicious transaction report to the Financial Intelligence Unit.

Article 20 - Other Higher Risk Customers

20.1 Banks and financial institutions shall conduct enhanced customer due diligence for all categories of higher risk customers, including those high risk customers mentioned in articles 18 and 19 of the present Prakas, to ensure that banks and financial institutions are not abused by money launderers and financiers of terrorism.

20.2 Enhanced due diligence should include at least:

- more detailed information from the customer, in particular, on the purpose of the business relationship and source of funds;
- independent research and sourcing of additional information about the customer; and
- approval by senior management.

Article 21 - Existing Accounts

21.1 Banks and financial institutions should take necessary measures to ensure that the records of existing customers remain up-to-date and relevant. Further evidence of the identity of existing customers should, where necessary, be obtained to ensure compliance with customer due diligence standards set by the present Prakas.

21.2 Banks and financial institutions should conduct regular reviews on existing records of customers. These reviews should at least, be conducted when:

- a significant transaction is to take place;
- there is a material change in the way the account is operated;
- the customer's particulars change substantially; or
- information held on the customer is insufficient.

21.3 In the event that the circumstances above do not arise, banks and financial institutions should, based on risk assessment, obtain additional information in line with their current standards from those existing customers that are of higher risk.

Article 22 – Record keeping

22.1 Banks and financial institutions should keep all records, documents and copies of documents involved in all forms of transactions for at least 5 years after the date of the transaction. All identification data, files, records, documents, business correspondence and copies of documents obtained on a customer must be maintained for at least 5 years after the accounts have been closed or the business relations with the customer have ended.

22.2 Where the records are subjected to an on-going investigation or suspicious transaction report submitted, they shall be retained beyond the stipulated

retention period until it is confirmed by the relevant authority that such records are no longer needed.

Article 23 – Audit Trail

23.1 Banks and financial institutions must ensure that the retained documents and records are able to create an audit trail on individual transactions that would enable the supervisory and enforcement agencies to trace funds.

23.2 The records kept must enable banks and financial institutions to establish the history and nature of and reconstruct each transaction. The records shall include at least:

- the origin of funds, such as method of receipt and or name of originator of wire transfer;
- the identity of the person undertaking the transaction if not an account holder;
- the type of transaction; and
- the instruction and the destination of fund transfers.

Article 24 – Record Format

Banks and financial institutions should retain the relevant document as originals or copies, on microfilm or in electronic form, provided that such forms are secured and retrievable upon request and provided in an accurate and timely manner

Article 25 – On-Going Monitoring

25.1 Banks and financial institutions should conduct on-going due diligence for all customer relationships, using a risk-based approach. The risk-based approach to on-going customer due diligence should ensure that the risk profile of the customer is up-to date.

25.2 Banks and financial institutions shall pay special attention to all complex, unusual large transactions, or unusual patterns of transactions, to determine whether the transactions have an apparent or visible or lawful purpose.

Article 26 – Management Information System

Banks and financial institutions should put in place an adequate management information system for identifying and detecting transactions that they suspect or have reasonable grounds to suspect related to proceeds from an unlawful activity or the customer is involved in money laundering or financing of terrorism. The management information systems should provide banks and financial institutions timely information on a regular basis to enable them to detect suspicious activity.

Article 27 – Special Attention

Banks and financial institutions should conduct on-going due diligence with regards to business relationships and transactions with individuals, business, company and financial institutions from countries which have insufficiently implemented the internationally accepted AML/CFT measures. Such business relationships and transactions should require banks and financial institutions to make

further detailed inquiries, about their background and purpose, to establish the findings in writing, and to make them available to the competent authorities.

Article 28 – Cash Transaction Reporting

28.1 Banks and financial institutions are required to report to the Financial Intelligence Unit cash transactions exceeding USD 10,000 (or 40 million Riels or foreign currency equivalent).

28.2 Cash transactions shall be provided to the Financial Intelligence Unit, within 14 days of the date of the transaction and be submitted on the approved 'Cash Transaction Report' form issued by the Financial Intelligence Unit or using the approved format for electronic reporting. A copy of the approved Cash Transaction Report form is attached at Appendix IV.

28.3 Reportable cash transactions include multiple cash transactions for a customer / account where the total amount of the combined transactions exceeds USD 10,000 (or 40 million Riels or foreign currency equivalent) on any one day.

Article 29 – Suspicious Transaction Reporting

29.1 Banks and financial institutions are required to establish a reporting system and to promptly submit suspicious transaction reports to the Financial Intelligence Unit when any of its employees suspects or has reasonable grounds to suspect that the transaction involves proceeds of an offence or are related to money laundering or financing of terrorism or they have any other grounds of suspicion about a customer transaction. Some examples of suspicious transactions are listed in Appendix II of the present Prakas. These examples are not exhaustive and only provide examples of basic ways in which money may be laundered or used for the financing of terrorism. Banks and financial institutions should establish their own internal guidelines on suspicious transaction reporting incorporating the relevant provisions in the Law on Anti-Money Laundering and Combating the Financing of Terrorism and the relevant provisions in the present Prakas, including a list of suspicious transactions indicators.

29.2 Banks and financial institutions should also submit a suspicious transaction report when a new or existing customer fails to complete the customer due diligence without reasonable excuse, regardless of whether the bank or financial institutions accept, reject, continue or terminate the business relationship with such customer.

Article 30 - Reporting Mechanisms

30.1 Banks and financial institutions should appoint an officer at the senior management level to be the compliance officer responsible for the submission of suspicious transaction reports to the Financial Intelligence Unit. The appointed compliance officer should be the point of reference for the Financial Intelligence Unit. Banks and financial institutions should ensure that all suspicious transaction reports prepared by employees are properly channelled to the compliance officer.

30.2 The employees of banks and financial institutions should report suspicious transactions to the compliance officer even if they do not know precisely what the underlying unlawful activity is or whether such activities have occurred.

30.3 Once the suspicious transaction report reaches the compliance officer, the compliance officer should promptly evaluate and establish whether there are reasonable grounds for suspicion and promptly, within 24 hours, submit the suspicious transaction report to the Financial Intelligence Unit unless the compliance officer considers, and records his/her opinion, that such reasonable grounds do not exist.

30.4 The suspicious transaction report submitted by the compliance officer shall be in writing and using the approved form as attached in Appendix III and delivered by safe hand, secure mail or secure electronic transmission to Financial Intelligence Unit.

30.5 Banks and financial institutions should ensure that when preparing and submitting a suspicious transaction report, information about the suspicious transaction, the customer and the reporting of the matter remains confidential and is available only to staff, on a strict 'need to know' basis.

30.6 Banks and financial institutions should authorise their compliance officer to cooperate with the Financial Intelligence Unit in providing additional information and documentation requested and to address further enquiries with regard to the submitted suspicious transaction report.

Article 31 - Prohibition of Tipping Off

31.1 Banks and financial institutions must ensure that the reporting system put in place for the submission of suspicious transaction reports is operated in a confidential manner.

31.2 Banks and financial institutions must ensure that the customer reported on, is not informed of the existence of the suspicious transaction report or does not become aware of such suspicious transaction report. Staff should be made aware that article 15 of the Law on Anti-Money Laundering and Combating the Financing of Terrorism prohibits any individual having knowledge of a suspicious transaction report from communicating such information or reports to any natural or legal persons other than the FIU, except where so authorized by the FIU.

Article 32 - Others Issues

32.1 Banks and financial institutions should maintain a complete file on all suspicious transaction reports submitted by their employees to its compliance officer and such reports that have been further submitted to the Financial Intelligence Unit.

32.2 Banks and financial institutions must take reasonable measures to ensure that all their officers and employees involved in conducting or facilitating customer transactions are aware of these reporting procedures.

Article 33 – Detection and Reporting of the Financing of Terrorism

33.1 Banks and financial institutions should take the necessary measures to ensure compliance with the United Nations Security Council (UNSC) Resolutions and relevant regulations and legislation on financing of terrorism.

33.2 Banks and financial institutions should extend the suspicious transaction report system and mechanism to cover suspicion of financing of terrorism.

33.3 Banks and financial institutions should maintain a database of names and particulars of terrorist in the United Nations list and they should consolidate their database with the other recognised lists of designated persons. Information contained in the database should be updated and relevant and made easily accessible to employees for the purpose of identifying suspicious transactions and freezing accounts / funds.

33.4 Banks and financial institutions should conduct checks of the names of new and existing customers against the names in the database. If there is a name match, the banks and financial institutions should take reasonable measures to verify and confirm the identity of its customer. If the customer and the person listed in the database are the same person, the bank or financial institution should immediately freeze the customer's accounts and inform the Financial Intelligence Unit. Where banks and financial institutions suspect that a transaction is terrorist-related, it should make a suspicious transaction reports to the Financial Intelligence Unit.

Article 34 – Risk Management

34.1 The Board of Directors of banks and financial institutions should establish an effective internal control system for AML/CFT compliant with legal and regulatory requirements. It is responsibility of the senior management to ensure such internal controls are implemented effectively.

34.2 The Board of Directors and senior management should be aware of and understand the AML/CFT measures required by law, the regulators, the industry's standards and best practices as well as the importance of putting in place AML/CFT measures to prevent their bank or financial institution from being abused by money launderers and financiers of terrorism. The Board of Directors should oversight the overall AML/CFT measures undertaken by the bank or financial institution.

34.3 The Board of Directors and senior management should be aware of the money laundering and financing of terrorism risks associated with all its business products and services.

34.4 The Board of Directors should ensure that its bank or financial institution has, at the minimum, policies on AML/CFT procedures and controls. The senior management should assist the Board of Directors in formulating the policies and ensure that the policies are in line with the risks associated with the nature of business, and complexity and volume of the transactions undertaken by the bank or financial institution.

34.5 The Board of Directors should ensure that the procedures for AML/CFT measures including those required for customer acceptance policy, customer due diligence, record keeping, on-going monitoring, reporting of suspicious transactions and combating the financing of terrorism are in place.

34.6 The Board of Directors should assess the implementation of approved AML/CFT policies by the senior management via periodic reports.

34.7 The Board of Directors should define the lines of authority and responsibilities for implementing the AML/CFT measures and ensure that there is a separation of duty between those implementing the policies and procedures and those enforcing the controls. The Board of Directors should ensure the:

- ❖ appointment of a compliance officer to ensure that the policies, procedures and controls are in place; and
- ❖ effectiveness of internal audit in assessing and evaluating the controls in place to counter money laundering and financing of terrorism.

34.8 The Board of Directors should review and assess the policies and procedures on the AML/CFT measures in line with changes and developments in its products, services and technology systems, as well as trends in money laundering and financing of terrorism techniques. The senior management should implement the necessary changes to the policies and procedures with the approval of the Board of Directors to ensure that the current policies are sound and appropriate.

34.9 The Board of Directors and senior management should ensure that there are adequate ongoing AML/CFT training programs in place.

Article 35 - Staff Integrity

Senior management should ensure that its bank or financial institution establish an employee assessment system, approved by the Board of Directors, to adequately screen its employees, both existing and new, to ensure that the integrity of its employees is not compromised. The employee assessment system should at least examine personal information including criminal records, employment and financial history of its new employees as part of the recruitment process.

Article 36 - Compliance Officer

36.1 Senior management is responsible to appoint the compliance officer at senior management level with the approval of the Board of Directors. Senior management should ensure that the compliance officer effectively discharges his/her AML/CFT responsibilities. The compliance officer should act as the reference point for the AML/CFT measures the bank or financial institution has established, including employee training and reporting of suspicious transactions.

36.2 Banks and financial institutions should upon the appointment or change in the appointment of the compliance officer inform the Financial Intelligence Unit of the details of the compliance officer including the name, address, telephone number, facsimile number, e-mail address and other relevant background.

36.3 Banks and financial institutions should ensure that the roles and responsibilities of the compliance officer are clearly defined and documented. The roles and responsibilities of the AML/CFT compliance officer should include at least ensuring:

- ❖ implementation of the policies for AML/CFT measures;
- ❖ the appropriate AML/CFT procedures including customer acceptance policy, customer due diligence, record keeping, on-going monitoring, reporting of suspicious transactions and combating the financing of terrorism are implemented effectively;
- ❖ regular assessment of the AML/CFT mechanisms to ensure that the mechanisms are sufficient to address the changing trends;

- ❖ the channel of communication from the respective employees to the compliance officer is secured and that any information is kept confidential;
- ❖ compliance with the AML/CFT legal and regulatory requirements;
- ❖ all employees are aware of AML/CFT measure including policies, control mechanisms and channel of reporting to ensure the effectiveness of such measures;
- ❖ the identification of money laundering and financing of terrorism risks associated with new products or services or arising from the bank's or the financial institution's operational changes, including the introduction of new technology and processes.

36.4 Compliance officers should have the necessary knowledge and expertise to effectively discharge his/her responsibilities, including knowledge on AML/CFT obligations required under the relevant laws and regulations and an understanding of developments in money laundering and financing of terrorism techniques

Article 37 - Staff Training and Awareness Programmes

37.1 Banks and financial institutions should have an awareness and training programme on AML/CFT practices and measures for its employees. The training and awareness programme must be extended to all new and existing employees.

37.2 Senior management should ensure that proper channels of communication are in place to inform all levels of employees in banks and financial institutions of their AML/CFT policies and procedures.

37.3 Employees should be aware of AML/CFT policies and controls in place and the requirements as specified in the present Prakas and in banks and financial institutions AML/CFT internal manual.

37.4 The AML/CFT internal manual should at least contain the following:

- ❖ the *Law on Anti-Money Laundering and Combating the Financing of Terrorism*;
- ❖ the present Prakas;
- ❖ the FATF Forty plus Nine Recommendations;
- ❖ the Customer Due Diligence Paper by Basel Committee on Banking Supervision; and
- ❖ the bank's and financial institution's measures to meet all AML/CFT requirements.

37.5 Banks and financial institutions should at least adapt to their needs the following training packages for the various sectors of employees within their institutions:

- ❖ *New Employees*
  A general background to money laundering and financing of terrorism, the requirement and obligation to identify and report suspicious transactions to the appropriate designated point within banks and financial institutions, and the importance of not tipping off the customer.

- ❖ *Front-Line Employees*

Employees who deal directly with the customers as the first point of contact with potential money launderers and financiers of terrorism should be trained in identifying suspicious transactions, the measures to be taken once a transaction is deemed to be suspicious, factors that may give rise to suspicions, large cash reporting and enhanced customer due diligence.

- *Employees - Account Opening/New Customers*
  Employees, who are responsible for account opening or the acceptance of new customers, should at least receive the equivalent training given to front-line employees. In addition, they should be trained in customer identification and verification, opening of accounts and establishing business relationship with customers.

- *Supervisors and Managers*
  Supervisors and managers should receive a higher level of instruction covering all aspects of AML/CFT procedures including the penalties for non-compliance to the AML/CFT requirement, and procedures in addressing combating the financing of terrorism issues.

37.6 These training and awareness programmes should be conducted regularly with refresher courses provided for employees. New employees should be trained within three months of commencement of employment and front line employees, supervisors and managers should have refresher training annually.

Article 38 - Internal Audit

38.1 The Board of Directors should ensure that internal auditors undertake audit of the effectiveness and compliance with AML/CFT requirements of the relevant laws and regulation as well as the present Prakas.

38.2 The Board of Director should ensure that the roles and responsibilities of the internal auditor are clearly defined and documented and at least include:

- testing the effectiveness of the policies, procedures and control for AML/CFT measures;
- ensuring effectiveness of AML/CFT control mechanisms including the appointment of compliance officers, staff training and awareness programmes, employee screening mechanisms and AML/CFT internal manual; and
- ensuring that measures put in place are in line with current developments and changes of the relevant AML/CFT requirements.

38.3 Banks and financial institutions should inform the Financial Intelligence Unit and the National Bank of Cambodia upon the appointment or change in the appointment of the internal auditor and on the approach and procedures adopted by the internal auditors.

38.4 The internal auditor should submit a written report on the audit findings to the Board of Directors on a regular basis. The annual audit report should highlight inadequacies of any AML/CFT measures and control systems within the bank or the financial institution, and the Board of Directors should ensure that necessary steps are taken to rectify the situation. Audit findings and reports on AML/CFT should be submitted to the National Bank of Cambodia after consideration by the Board of Directors.

Article 39 -

The present Prakas supersedes the existing Prakas on Standardised Procedures for Identification of Money Laundering at the Banking and Financial Institution issued on October 21, 2002 and Circular on Suspicious Transactions and Know your Customer Policies issued on October 04, 2003.

Article 40 -

The General direction, the General Secretariat, the General Inspection, the General Cashier and all departments of the National Bank of Cambodia, all Banking and Financial Institutions under NBC's supervisory authority shall strictly implement the present Prakas.

Article 41-

The present Prakas shall have effect from the signing date.

Phnom Penh, May 30, 2008

Governor
Signed : Chea Chanto

cc:
- All members of the Board of Directors
- The parties concerned as stated in article 40
- File
- CM "for info"
- Administration Department of CM "for publication in the National Gazette"

Appendix I

DESCRIPTION OF MONEY LAUNDERING AND FINANCING OF TERRORISM

Pursuant to the Law on Anti-Money Laundering and Combating the Financing of Terrorism

"*Money laundering*" shall mean:

1. The conversion or transfer of property, knowing that such property is the proceeds of offence, for the purpose of concealing or disguising the illicit origin of the property or of helping any person who is involved in the commission of the predicate offence to evade the legal consequences of his or her action;

2. The concealment or disguise of the true nature, source, location, disposition, movement or ownership of or rights with respect to property, knowing that such property is the proceeds of offence;

3. The acquisition, possession or use of property, knowing, at the time of receipt, that such property is the proceeds of offence;

4. Participation in, and attempts to commit and aiding and abetting, any of the acts defined in accordance with this article;

"Financing of terrorism" shall mean:

"*Financing of terrorism*" shall mean the wilful provision or collection of funds, directly or indirectly, through whatever means, with the intention that such funds be used or in the knowledge that they are or may be used, in full or in part, for the purpose of supporting terrorism, terrorist acts or terrorist organizations.

Appendix II

EXAMPLES OF SUSPICIOUS TRANSACTIONS

Cash Transactions, Deposit and Withdrawal

1. Unusually large cash deposits made by an individual or company whose ostensible business activities would normally be generated by cheques and other instruments.
2. Substantial increases in cash deposits of any individual or business without apparent cause, especially if such deposits are subsequently transferred within a short period of time, out of the account and/or to a destination not normally associated with the customer.
3. Company accounts whose transactions, both deposits and withdrawals, are denominated in cash rather than the forms of debit and credit normally associated with commercial operations (e.g. cheques, Letters of Credit, Bills of Exchange, etc.)

4. Customers who constantly pay in or deposit cash to cover requests for bankers' draft, money transfers or other negotiable and readily marketable money instruments.

5. Customers who seek to exchange large quantities of low denomination notes for those of higher denomination.

6. Branches of banks and financial institutions that have a great deal more cash transactions than usual (Head Office statistics detect aberrations in cash transactions).

7. Customers whose deposits contain counterfeit notes or forged instruments.

8. Customers transferring large sums of money to or from overseas locations with instructions for payment in cash.

9. Purchasing or selling of foreign currencies in substantial amounts by cash settlement despite the customer having an account with the institution.

10. Customers making large and frequent cash deposits but cheques drawn on the accounts are mostly to individuals and firms not normally associated with their retail business.

11. Deposits for a business entity in combinations of monetary instruments that are atypical of the activity normally associated with such a business.

12. Mixing of cash deposits and monetary instruments in an account in which such transactions do not appear to have any relation to the normal use of the account.

13. Multiple transactions carried out on the same day at the same branch of a financial institution but with an apparent attempt to use different tellers.

14. The structuring of deposits through multiple branches of the same financial institution or by groups of individuals who enter a single branch at the same time.

15. The deposit or withdrawal of cash in amounts which fall consistently just below identification or reporting thresholds.

16. The customer presents funds that have not been counted and upon counting reduces the fund involved to an amount just below what would trigger reporting or identification requirements.

17. The deposit or withdrawal of multiple monetary instruments at amounts which fall consistently just below identification or reporting thresholds, particularly if the instruments are sequentially numbered.

Accounts

18. Accounts that appear to act as pass through accounts with high volumes of credits and debits and low average monthly balances.

19. Customers who wish to maintain a number of trustee or client accounts, which do not appear consistent with the type of business, including transactions, which involve nominee names.

20. 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.

21. Any individual or company whose account shows no normal personnel 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 and/or his business (e.g. a substantial increase in turnover on an account).

22. Reluctance to provide normal information when opening an account, attempts to reduce the level of information provided to the minimum or providing information that is difficult or expensive for banks and financial institutions to verify.

23. Customers who appear to have accounts with several bank and micro finance institutions within the same locality, but choose to consolidate monies from such accounts on regular basis for onward transmission of the funds to another 3rd party account.

24. Paying in large third party cheques endorsed in favour of the customer.

25. An inactive account containing a minimal sum suddenly receives a deposit or series of deposits followed by daily cash withdrawals that continue until the transferred sum has been removed.

26. Greater use of safe deposit facilities, which does not commensurate with the customer profile.

27. Customer avoiding contact with employees of banks and financial institutions for transaction.

28. Substantial increases in deposits of cash or negotiable instrument 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's company and trust accounts.

29. Customers who decline to provide information that in normal circumstances would make the customer eligible for credit or for other banking services that would be regarded as valuable.

30. Large number of individuals making payment into the same account without an adequate explanation.

31. High velocity of funds through an account, i.e., low beginning and ending daily balances, which do not reflect the large volume of dollars flowing through an account.

32. An account opened in the name of a money-changer that receives structured deposits (e.g. constant amount of deposit regularly).

33. An account operated in the name of an off-shore company with structured movement of funds.

34. Accounts that receive relevant periodical deposits and are inactive at other periods. These accounts are then used in creating a legitimate appearing financial background through which additional fraudulent activities may be carried out.

35. An account for which several persons have signature authority, yet these persons appear to have no relation among each other (either family ties or business relationship).

36. An account opened by a legal entity or an organisation that has the same address as other legal entities or organisations but for which the same person or persons have signature authority, when there is no apparent economic or legal reason for such an arrangement (for example, individuals serving as company directors for multiple companies headquartered at the same location, etc.).

37. An account opened in the name of a recently formed legal entity and in which a higher than expected level of deposits are made in comparison with the income of the founders of the entity.

38. An account opened in the name of a legal entity that is involved in the activities of an association or foundation whose aims are related to the claims or demands of a terrorist organisation.

39. An account opened in the name of a legal entity, a foundation or an association, which may be linked to a terrorist organisation and that shows movements of funds above the expected level of income.

International Banking/Trade Finance

40. Customer introduced by an overseas branch, affiliate or other bank based locations of specific concern (for example, countries where production of drugs or drug trafficking may be prevalent, countries designated by national authorities, FATF's non-cooperative countries and territories, etc.).

41. Use of Letter of Credit and other methods of trade finance to move money between countries where such trade is not consistent with the customer's usual business.

42. Customers who make regular and large payments, including wire transactions, that cannot be clearly identified as bona fide transactions, or receive regular and large payments from countries which are commonly associated with the production, processing or marketing of drugs, prescribed terrorist organizations or tax havens.

43. Building up of large balance, not consistent with the known turnover of the customer's business, and subsequent transfer to account(s) held overseas.

44. Unexplained electronic fund transfers by customers on an in-and-out basis or without passing, through an account.

45. Frequent requests for or paying in of travellers' cheques or foreign currency drafts or other negotiable instruments to be issued or originating from overseas.

46. Customers sending and receiving wire transfer to/from tax haven countries, particularly if there are no apparent business reasons for such transfers or such transfers are not consistent with the customers' business or history.

Banks and financial institutions employees and agents

47. Changes in employee characteristics, e.g. lavish life styles or avoiding taking holidays.

48. Changes in employee or agent performance, e.g. the salesman selling products for cash has a remarkable or unexpected increase in performance.

49. Any dealing with an agent where the identity of the ultimate beneficiary or counterpart is undisclosed, contrary to normal procedure for the type of business concerned.

50. Sudden strong performance by employees in special relationship/confidential relationship banking services such as trust or private banking services or sudden increase in the wealth/spending of such employees.

Private banking and trust services

51. The grantors of private banking and trust accounts that direct loans from their accounts to other parties or business interests of account principals or beneficiaries.

Secured and Unsecured Lending

52. Customers who repay problem loans unexpectedly.

53. Request to borrow against assets held by banks and financial institutions or a third party, where the origin of the assets is not known or the assets are inconsistent with the customer's standing.

54. Request by a customer for a bank and micro finance institution to provide or arrange financial contribution to a deal which is unclear, particularly, where property is involved.

55. Customers who unexpectedly repay in part or full a mortgage or other loan in a way inconsistent with their earning capacity or asset base.

Wire transfer

56. Wire transfers ordered in small amounts in an apparent effort to avoid triggering identification or reporting requirements.

57. Wire transfers to or for an individual where information on the originator, or the person on whose behalf the transaction is conducted, is not provided.

58. Use of multiple personal and business accounts or the accounts of non-profit organisations or charities to collect and then funnel funds immediately or after a short time to a small number of foreign beneficiaries.

Characteristic of customer or his business activity

59. Funds generated by a business owned by individuals or involved by multiple individuals of the same origin from countries of specific concern acting on behalf of similar business types.

60. Shared address for individuals involved in cash transactions, particularly when the address is also a business location and/or does not seem to correspond to the stated occupation (for example student, unemployed, self-employed, etc.).

61. Stated occupation of the customer does not commensurate with the level or type of activity (for example, a student or an unemployed individual who receives or sends large numbers of wire transfers, or who makes daily maximum cash withdrawals at multiple locations over a wide geographic area).

62. Regarding non-profit or charitable organisations, financial transactions for which there appears to be no logical economic purpose or in which there appears to be no link between the stated activity of the organisation and the other parties in the transaction.

63. Unexplained inconsistencies arising from the process of identifying or verifying the customer (for example, regarding previous or current country of residence, country of issue of the passport, countries visited according to the passport, and documents furnished to confirm name, address and date of birth).

Transaction linked to locations of concern

64. Deposits are followed within a short time by wire transfers of funds, particularly to or through a location of specific concern (for example, countries designated by national authorities, FATF non-cooperative countries and territories, etc.).

65. A business account through which a large number of incoming or outgoing wire transfers take place and for which there appears to be no logical business or other economic purpose, particularly when this activity is to, through or from locations of specific concern.

66. A customer obtains a credit instrument or engages in commercial financial transactions involving movement of funds to or from locations of specific concern when there appears to be no logical business reasons for dealing with those locations.