ශ්‍රී ලංකා මහ බැංකුව
இலங்கை மத்திய வங்கி
CENTRAL BANK OF SRI LANKA

ජනාධිපති මාවත,
තැපැල් පෙට්ටිය 590,
කොළඹ 1, ශ්‍රීලංකාව.
විදුලි පුවත්: 'මහබැංකුව'

ஜனாதிபதி மாவத்தை,
த. பெ. இல. 590,
கொழும்பு - 1. ஸ்ரீ லங்கா
தந்தி : 'மத்தியவங்கி'

Janadhipathi Mawatha,
P.O. Box 590,
Colombo 1, Sri Lanka.
Telegrams: 'CENTRABANK'

Our Ref: 37/03/004/0003/007

Financial Intelligence Unit
Tel. No. 2477125
Fax No: 2477692
e-mail: fiu@cbsl.lk

28th December 2007

The Chief Executive Officer

Dear Sir/Madam,

MANDATORY KNOW-YOUR-CUSTOMER AND CUSTOMER DUE DILIGENCE (KYC/CDD) RULES FOR THE SECURITIES INDUSTRY IN TERMS OF THE PROVISIONS OF THE FINANCIAL TRANSACTIONS REPORTING ACT NO. 6 OF 2006 (FTRA)

Detailed guidance and rules based on international best practices and also where relevant, incorporating recommendations by the Securities and Exchange Commission of Sri Lanka are enclosed herewith.

You are advised to ensure that a proper policy framework and operations guidelines to give effect to the guidance and the rules so prescribed are in place within a specific AML/CFT policy developed by your institution for this purpose.

You are required to submit quarterly reports to the FIU on the last date of the quarterly period using the attached format at annexure 1. You are also required to ensure that your institution, as a securities market participant, is fully compliant with these rules, and inform us of the progress made by 31st January 2008.

These rules are issued under Section 2(3) of the Financial Transactions Reporting Act No.6 of 2006, and any contravention or non-compliance with the rules so prescribed will be liable to penalties as prescribed in the relevant provisions of the Act.

Yours faithfully,

H A Karunaratne
Actg. Director (FIU)

Copy to: Director General, Colombo Stock Exchange,
Level 4-04, World Trade Centre, Colombo 1

RULES ON
KNOW YOUR CUSTOMER (KYC) & CUSTOMER DUE DILIGENCE (CDD)
FOR THE SECURITIES INDUSTRY

Introduction

Public confidence in financial institutions, and hence their stability, is enhanced by sound practices that reduce financial risks to their operations. Money laundering and terrorist financing can harm the soundness of a country's financial system, as well as the stability of individual financial institutions, in multiple ways. Customer identification and due diligence procedures also known as "know your customer" rules, are part of an effective AML/CFT regime. These rules are not only consistent with, but also enhance, the safe and sound operation of banking and other types of financial institutions.

While preparing operational guidelines on customer identification and due diligence procedures, institutions are advised to treat the information collected from the customer for the purpose of opening of accounts, as confidential and not divulge any details thereof for cross-selling or for any other purposes, and that the information sought is relevant to the perceived risk, is not intrusive and is in conformity with the rules issued hereunder.

The mandatory rules on KYC/CDD include the following sections:

Part I - General Rules

Part II - Specific Rules

Part III - Specific Customer Identification

Part IV - Declaration Format

Part V - Suspicious Transaction Report Format/Instructions

These rules are issued under Section 2(3) of the Financial Transactions Reporting Act No.6 of 2006 and any contravention of, or non-compliance with the same will be liable to the penalties under the relevant provisions of the Act.

Actg. Director
Financial Intelligence Unit,
Central Bank of Sri Lanka

28th December 2007

PART I
GENERAL RULES FOR THE SECURITIES INDUSTRY

A. ANTI-MONEY LAUNDERING PROGRAM

1. Introduction

An institution should develop and implement a written program reasonably designed to prevent it from being used for money laundering and terrorist financing. This program should be approved in writing by the directors of the company which carries out the business of broker/dealer/market intermediary or by the trustee/s of a unit trust. It should include:

- the establishment of policies, procedures, and internal controls;
- an ongoing employee training program;
- an independent audit function to test the program for compliance; and
- appropriate compliance management arrangements. The type and extent of measures to be taken for each of these requirements should be tailored with respect to the risk or vulnerability to money laundering and terrorist financing and the size, location, and activities of the business.

2. Policies and Procedures

Written policies and procedures should set forth clearly the details of the program, including the responsibilities of the individuals and departments involved. Policies, procedures, and internal controls should be reasonably designed to detect activities indicative of money laundering and to assure compliance with anti-money laundering legislation. An institution should monitor the operation of its program and assess its effectiveness. Customer identification and verification procedures, as well as procedures regarding the detection and reporting of suspicious activity, should be included as a part of the anti-money laundering program.

3. Employee Training

The training program for employees of the institution should provide both a general awareness of overall anti-money laundering legislation and money laundering issues, as well as more job-specific guidance regarding particular employees' roles and functions in the anti-money laundering program. For employees whose duties bring them in contact with anti-money laundering legislation or possible money laundering activity, training should occur when the employee assumes those duties, with subsequent periodic updates and refreshers.

4. Independent Audit

The institution should conduct periodic independent testing of its program to assess compliance with and the effectiveness of the program, and to assure that the program is functioning as designed. Such testing may be accomplished either by a qualified outside party, or by employees of the institution so long as those same employees are not involved in the operation or oversight of the programme. A written assessment or report should be a part of the review, and any recommendations should be promptly implemented or submitted to the directors of a fund company, general partner of a limited partnership, or trustee of a unit trust for consideration.

5. **Compliance Management**
The institution should charge an individual (or group of individuals) with the responsibility for overseeing the anti-money laundering program. The person (or group of persons) should be knowledgeable regarding anti-money laundering legislation and money laundering issues and risks, and empowered with full responsibility and authority to develop and enforce appropriate policies and procedures throughout.

6. **Financial Services Groups and Anti-Money Laundering Programs**
An institution often is part of a large financial services group. These groups may choose to establish an anti-money laundering program that applies to all institutions that they sponsor, operate or advise. Further, large financial services groups that have banks, broker/dealers or insurance companies as their core business may already have in place an anti-money laundering program that applies to all companies within the group. A financial services group may utilize the group's anti-money laundering program, so long as every institution is covered by an anti-money laundering program containing the four elements set forth above. Each institution– through its board of directors, general partner or trustee - should have clear written documentation indicating that it has adopted an anti-money laundering program.

B. CLIENT IDENTIFICATION AND VERIFICATION PROCEDURES

An institution may apply client verification procedures on a risk-sensitive basis. An institution should establish the bases for such risk determinations and should be able to justify its assessments to its regulator.

1. **Responsibility for client identification and verification**
An institution has a responsibility for verifying the identity of the investor, and the beneficial owner of the investor when it is apparent that an account is beneficially owned by a party other than the investor, and performing more general "know your customer" procedures following a risk-based approach. The general "know your customer" procedures, including obtaining information, such as financial background and business objectives, in order to develop a business and risk profile and to ensure that transactions being conducted are consistent with that profile (including, where necessary, the client's source of funds).

2. **Verifying investor identity**
Measures to identify and verify the identity of the investor, and the beneficial owner of the investor when it is apparent that an account is beneficially owned by a party other than the investor, to the extent reasonable and practicable, may be determined on a risk sensitive basis depending on the type of investor, business relationship or transaction, and the types of accounts opened by the institution. This applies to units sold or redeemed by the institution or through any market intermediary. The verification should provide a reasonable basis for an institution to believe that the true identity of the investor is adequately known. Where the risk that an institution will not know the true identity of an investor is higher (*e.g.*, accounts for politically exposed persons or entities with complex structures; accounts for nationals, residents, or entities from countries considered to be non-cooperative or inadequately regulated, etc.), an institution should apply more stringent client identification measures. Investor identification and verification processes should be properly documented in each case, and such records should be kept for at least six years after the business relationship has ended.

3. An institution may rely on documents as well as on non-documentary methods, or a combination of both, in order to identify investors and verify their identity. With respect to natural persons, reliable verification methods could include the following:

- An unexpired government-issued identification evidencing nationality or residence and bearing a photograph or other similar safeguards, such as a driver's license or passport;
- Independently verifying the investor's identity through the comparison of information provided by sources such as public database, or other sources;
- Checking references with other financial institutions;
- Obtaining account statements; and
- Face-to-face meetings; interviews; statements; home visits; references from previous business relationships. With respect to non-natural persons, reliable verification methods could include the following:
- Obtaining proof of incorporation or similar evidence of the legal status of the legal person or arrangement, as well as information concerning the investor's name, the names of trustees, legal form, address, directors, and documents evidencing the power of a person to bind the legal person or arrangement;
- Forming an understanding of the ownership and control structure; and
- Identifying the natural persons with a controlling interest and identifying the natural persons who comprise the management of the legal person or arrangement.

4. With respect to another institution, and/or a fund of funds, an institution need not verify the identity of the underlying beneficial owners of an investing Collective Investing Schemes (CIS) or fund of funds that:

- Is regulated or registered;
- Is based in a jurisdiction that the an institution is satisfied has appropriate anti-money laundering legislation;
- Has in place an anti-money laundering program; and
- Is supervised for, and has measures in place to comply with, CDD requirements.

5. **Timing of identification and verification**

An institution should identify the investor before or during the opening of an account or accepting an investment. An institution should verify identity as soon as possible, before or after the opening of an account or accepting an investment, for purposes of assuring that the risks are effectively managed. In this regard, it is essential not to interrupt the normal conduct of business.

Where the investor's identity has yet to be verified, an institution will need to adopt risk management procedures with respect to the conditions under which an investor may utilise the account or investment prior to verification. These procedures should include a set of measures such as a limitation of the number, types and/or amount of transactions that can be performed, and the monitoring of large transactions being carried out of expected norms for that type of relationship. Where it is not possible after reasonable efforts to verify the identity of an investor, an institution should consider halting transactions or terminating its relationship and also should consider making a Suspicious Activity Report to the appropriate authorities in relation to the investor. It may be appropriate for an institution to consult with its regulator and appropriate law enforcement agencies prior to halting transactions in a particular account or terminating its relationship with any investor.

6. **Potential low risk situations**

As noted above, the identity verification procedures of an institution may be risk-based depending on the type of investor, business relationship, or transaction. Where there are low risks, it may be appropriate for an institution to apply simplified verification procedures. These procedures, of course, must still be sufficient for the institution to achieve the goal of verification – establishing a reasonable belief that it knows the true identity of its investor.

In the event a broker firm/CDS obtains a confirmation from a bank which maintains a bank account for a client trading through a broker firm, to the effect that, when opening and maintaining the bank account, the bank has followed the KYC and CDD requirements, the broker firm/CDS may at its discretion considering the risk level of the client, waive off the above requirements to verify the source of funds received.

PART II

SPECIFIC RULES FOR THE SECURITIES INDUSTRY

1. **Introduction**

The broker/dealer firm/market intermediary must obtain sufficient evidence of the identity of any client as soon as reasonably practicable after it has contact with a client.

2. Any broker/dealer firm/market intermediary should not proceed further with the transaction if satisfactory evidence of identity has not been provided unless directed to do so by the Financial Intelligence Unit.

3. Every broker/dealer firm/market intermediary should take reasonable care to make and retain adequate records for 6 years.

4. For the avoidance of doubt, for each transaction the firm should retain a record of;
   - The name and address of its customers;
   - The name and address (or identification code) of its counter party,
   - The investment dealt in, including price and size;
   - Whether the transaction was a purchase or a sale;
   - The form of instruction or authority;
   - The account details and the form in which the funds were paid to the firm (including, in the case of cheques, sort code, account number and name);
   - The form and destination of payment made by the firm to the customer;
   - Whether the investments were held in safe custody by the firm or sent to the customer or to his order, and if so to what name and address;

5. Every broker/dealer firm/market intermediary shall conduct on-going due diligence on the business transactions with the customer to ensure that the transactions are consistent with the firm's knowledge of the customer, the customer's business risk and source of income.

6. Every broker/dealer firm/market intermediary shall report to the Financial Intelligence Unit:-

- Any act which the firm suspects is preparatory to an offence under the provisions of the Convention on the Suppression of Financing of Terrorism Act No. 25 of 2005; or
- Any transaction or attempted transaction which the firm has reasonable suspicion that it may relate to the commission of any unlawful activity in terms of the Financial Transactions Reporting Act No. 6 of 2006 and Prevention of Money Laundering Act No. 5 of 2006.

7. Every broker/dealer firm/market intermediary to appoint a Compliance Officer to be responsible for ensuring compliance with the requirements of the Financial Transactions Reporting Act No. 6 of 2006.

8. The Compliance Officer should establish and maintain procedures to

- Implement the customer identification requirements
- Implement procedures for record keeping
- Implement a process of monitoring the customer transactions
- Implement a system for reporting suspicious activity to the Financial Intelligence Unit
- Make employees aware of the law relating to money laundering and terrorist financing
- Screen all persons before hiring them as employees to ensure ML/TF risks are adequately addressed.

PART III

SPECIFIC CUSTOMER IDENTIFICATION INFORMATION REQUIREMENTS IN RELATION TO SECURITY BROKERS
INFORMATION TO BE SUBMITTED BY APPLICANTS TO OPEN A CDS ACCOUNT

1. Natural Persons (Individuals)

A. Residents

a) Full Name.
b) Nationality.
c) Occupation.
d) Permanent Residential Address.
e) Current Residential Address.(If different from above)
f) Address for correspondence (if different from Residential Address.)
g) Proof of residency – copies of any utility bills (Eg: electricity, water, telephone bills etc.) or such other proof.
h) Copy of National Identity Card (NIC) or Passport (in the event NIC is not available.) If both NIC/Passport is not available a copy of the Driving License should be submitted, together with an Affidavit confirming the fact that both NIC and Passport are not available.

i) Name, address and copy of NIC/Passport of person/s authorized to give instructions.

B. Non-residents

a) Full Name.
b) Nationality.
c) Occupation.
d) Permanent Residential Address
e) Current Residential Address.
f) Proof of residency – copies of any utility bills (Eg: electricity, water, telephone bills etc.) or such other proof.
g) Address for correspondence (if different from Residential Address.)
h) SIERA Account details with proof (where the applicant is a Non Resident.)
i) Copy of Passport.
j) Name, address and copy of NIC/Passport of person/s authorized to give instructions.

2. Corporate Bodies

a) Full name of the Corporate Body (Company/Statutory body/a body established under an Act of Parliament/Society.)
b) Registered address.
c) Address for correspondence (if different from Registered Address.)
d) Place of Incorporation / place where established.
e) SIERA Account details with proof (where the applicant is a Non-Resident.)
f) Names, addresses, National Identity Card/Passport number/s and occupations of Directors. (If the company is listed in a Stock Exchange only the names should be given. Proof of such listing should be submitted in that event)
   If the Director/s is/are also a company, the following information on such Director company should be given:
   (i) Name of the company.
   (ii) Date of Incorporation.
   (iii) Place of Incorporation.
   (iv) Registered Address.
   If an authorized person is signing the CDS application form on behalf of the applicant company, a copy of the Board Resolution/Power of Attorney authorizing such person to sign on behalf of the Company and a copy of National Identity Card/Passport of such person should be submitted.
g) Names and addresses of top 10 shareholders/members. (Not applicable if the Company is listed in a Stock Exchange.)
h) Name of person/s authorized to give instructions with a copy of the Power of Attorney/Board Resolution.
i) Copies of following documents:
   (i) Articles of Association or corresponding document.
   (ii) Certificate of Incorporation or corresponding document.
   (iii) If a director/s of the applicant is/are also a company Certificate of Incorporation of such company.

(iv) Where the applicant is a Non-Resident, a copy of the Certificate of Good Standing issued by the Registrar of Companies/applicable authority where the Company is incorporated.

(v) Certified extract of the resolution to open the CDS account (in the alternative, the resolution may be certified in the CDS Account Opening Application itself).
Where the application is titled in the names of the 'Registered Holder/Global Custodian/Beneficiary' and forwarded through a Custodian Bank, a copy of the SWIFT message or similar document issued by the Global Custodian instructing the local Custodian Bank to open the account on behalf of the beneficiary Company should be submitted together with a declaration from the Global Custodian that a Custody arrangement or agreement exists between the Global Custodian and the beneficiary.

vi) Certificate to commence business. (where relevant.)

3. Funds approved by SEC

a) Name of the Fund.
b) Purpose of the Fund.
c) Place of establishment of the Fund.
d) Details (name, address, description etc.,) of the Trustee/Manager of the Fund .
e) If the Trustee/Manager is a company, date of incorporation, place of incorporation, registered address of such Trustee/Manager.
f) Copies of the documents relating to the establishment and management of the Fund (eg:Prospectus/Trust Deed/Management Agreement/Bankers/ Auditors).
g) Copy of the Letter of Approval of the Fund issued by the Supervisory Authority of the relevant country.
h) Copy/copies of the relevant Custody Agreement/s.
i) Details of Beneficiaries.

4. Certification

All supporting documents to be submitted to the CDS should be certified or attested or authenticated for purposes of validating by persons mentioned under (a) or (b) below. Such certification should state that the document certified is a true copy.

a) <u>Certification for Non Resident Applicants</u>

1) By the Company Registry or similar authority, where the documents were originally issued (applicable for Corporate Bodies), <u>or</u>
2) By a Sri Lankan diplomatic officer or Sri Lankan consular officer in the country where the documents were originally issued, <u>or</u>
3) By a Solicitor, Attorney-at-Law, Notary Public, practicing in the country where the applicant resides, <u>or</u>
4) Custodian Bank, <u>or</u>
5) Global Custodian – The Custodian Bank should certify the authenticity of the signature of the Global Custodian <u>or</u>
6.) Broker. (Applicable only in respect of Individuals.)

a) **Certification for Resident Applicants**

1) Registrar General of Companies or the Company Secretary (applicable in respect of Corporate Bodies), or
2) Attorney-at-Law / Notary Public, or
3) Broker, or
4) Custodian Bank.

NOTE:
The person certifying should place the signature, full name, address, contact telephone numbers and the official seal (Not applicable for Brokers, Custodian Banks and Global Custodians).

PART IV

THE FOLLOWING DECLARATIONS SHOULD BE SUBMITTED BY APPLICANTS TO OPEN A CDS ACCOUNT

- A declaration that the securities to be purchased through the CDS Account to be opened would be for the benefit of the applicant only and for no other beneficial owner/s. In the alternative, if the applicant is acting in the capacity of a Trustee, a declaration that the account is opened for the benefit of beneficiaries and declares the names, addresses and the nationalities, where the number of beneficiaries is up to three (3) only. If above such number, a declaration that information such as names, addresses & nationality pertaining to the ultimate beneficiaries of the account, are maintained with the applicant and an undertaking to release such information to CDS at any time upon request by the CDS.[CDS (1)A/CDS 2(A)]

- A declaration that the funds to be invested through the CDS will not be funds generated from any money laundering activity nor funds generated through the financing of terrorist or any other illegal activity. [CDS 1(A)/CDS 2(A)]

- A declaration that all the information given is true and accurate, and that no alteration, modification was made to the said information. [CDS 1(A)/CDS 2 (A)]

- A declaration that in the event of a variation of the information submitted to CDS, the applicant would inform the CDS, in writing, within 14 days of such change. [CDS 1(A)/CDS 2(A)]

- A declaration as set out in Appendix A below.

Appendix A
Declaration

I/We declare that I/we have not been banned and/or rejected and /or suspended by any criminal/civil tribunal or administrative authority in Sri Lanka or in any other country in connection with the following offences:

- Engaging directly or indirectly in any transaction in relation to any property which is derived or realized directly or indirectly, from any unlawful activity or from the proceeds of any unlawful activity as defined by the Financial Transactions Reporting Act No. 6 of 2006;
- Receiving, possessing, concealing, disposing, of or bringing into Sri Lanka or into any other country, or for investing in Sri Lanka or in any other country, any property which is derived or realized, directly or indirectly, from any unlawful activity or from the proceeds of any unlawful activity referred to above; or
- Any other offence which has been defined as an offence under the Prevention of Money Laundering Act No.5 of 2006 and any amendment thereto or any similar legislation in any other part of the world.

I/We hereby further declare that I/We am/are person(s) of good standing with no record of criminal convictions in relation to the offences stated above, in Sri Lanka or in any other country.

I/We hereby further declare that I/We or any persons(s) associated with me/us and/or any entity connected to me/us (as a partner, shareholder, director) have against me/us or persons connected and/or associated as aforesaid any convictions/pending criminal proceeding in Sri Lanka or in any other part of the world except the following (give detailed description of any pending litigation);

- ....
- ....
- ....
- ....

I/We declare that my/our application and other relevant documentation to open a CDS account has not been refused or any business relationship has not been declined previously by any other Participant Custodian, Bank Firm of the CDS/CSE.

I/We further declare and agree that, should the CSE/CDS determine any statements made by me/us herein to the contrary, (or any such matter through publicly available information or otherwise) which would in the opinion of the CSE/CDS be detrimental to the CDS as an institution having to comply with the laws/regulations of Sri Lanka pertaining to transactions of its account holders or parties connected to such account holders, the CDS is hereby authorized to unilaterally terminate all depositary and such other services connected to me/us and recover related costs or other expenses pertaining to this account.

PART V

SUSPICIOUS TRANSACTIONS REPORT (STR) FOR SECURITIES INDUSTRY IN TERMS OF THE FINANCIAL TRANSACTIONS REPORTING ACT NO. 6 OF 2006

Please note that to be accepted as a STR, this form must be completed in all material detail.

a. This report is made pursuant to the requirement to report suspicious transactions under the Financial Transactions Reporting Act No.6 of 2006 (FTRA).

b. Under section 12 of the FTRA, no civil, criminal or disciplinary proceedings shall be brought against a person who makes a report unless it was made in bad faith.

In accordance with Section 7 of the Financial Transactions Reporting Act No. 6 of 2006, the reporting entity is obliged to report suspicious transactions as soon as is practicable but no later than 2 working days to the Financial Intelligence Unit.

Please take note of the following prior to completing the Suspicious Transaction Report ("STR"):

- **Provide** a clear and concise description of the STR, and **state** all available information.
- **Document** in detail why the **transaction** is considered extraordinary, irregular or **suspicious.**
- **Provide** supporting documents where it is necessary to explain the STR.
- **Indicate** if the potential violation is an initial report or if it relates to a previous **transaction** or transactions reported.
- **Complete** this STR in Block letters.
- Take reference to the explanatory notes at page 16.

SUSPICIOUS TRANSACTIONS REPORT (STR) FOR SECURITIES INDUSTRY IN TERMS OF THE FINANCIAL TRANSACTIONS REPORTING ACT NO. 6 OF 2006

a. This report is made pursuant to the requirement to report suspicious transactions under the Financial Transactions Reporting Act No.6 of 2006 (FTRA).

b. Under section 12 of the FTRA, no civil, criminal or disciplinary proceedings shall be brought against a person who makes a report unless it was made in bad faith.

Name of the Reporting Company :.....

Date of Reporting :.....

Details of Disclosing Organization

Name of Organization	Registered Address

Person Subject of Disclosure:

Full Name	NIC/Passport Number/Address

OR Company Subject of Disclosure:

Company Name	Registered Address
Other information not covered above	

Financial Summary Overview:

Institution Name	

Financial Summary Details:

Date	
Value	

Date	
Value	

Date	
Value	

Date	
Value	

Date	
Value	

Date	
Value	

Associated Person (with Subject of Disclosure):

Full Name	NIC/Passport Number/Address

OR

Associated Company (with Subject of Disclosure):

Company Name	Registered Address
Other information not covered above	

Generic Reporting Form

Reason for suspicion

Use additional sheets if there are further details to be shown.

PART E: DETAILS OF REPORTING OFFICER & COMPLIANCE OFFICER

36. Date of Reporting: ☐☐ ☐☐ 2 0 0 ☐
D D M M YY Y Y

Reporting Officer: .....

.....

Name: ..... **Name of Compliance Officer**

Designation:.....

Address: .....

Contact No. ..... E-mail..... Fax .....

.....

Signature of Compliance Officer

PART E: FOR FIU OF SRI LANKA USE ONLY

Receiving Officer

Date Received: ☐☐ ☐☐ 2 0 0 ☐
D D M M Y Y Y Y

STR No: ☐☐☐☐☐☐☐☐☐☐

Date of Acknowledgement: ☐☐ ☐☐ 2 0 0 ☐
D D M M Y Y Y Y

FIU ACKNOWLEDGEMENT

Received by the Financial Intelligence Unit of the Central Bank , STR No. ☐☐☐☐☐☐☐☐☐

dated ☐☐ ☐☐ 200 ☐

from.....

.....

Director/FIU

GENERAL INSTRUCTIONS

Under the **FINANCIAL TRANSACTIONS REPORTING ACT, NO. 6 OF 2006 (FTRA)**, every reporting institution shall furnish details of suspicious transactions defined in Section 7 (1) of the FTRA.

7 (1) Where an Institution: -

a) has reasonable grounds to suspect that any transaction or attempted transaction may be related to the commission of any unlawful activity or any other criminal offence; or

b) has information that it suspects may be relevant ---

(i) to an act preparatory to an offence under the provision of the Convention on the Suppression of Financing of Terrorism Act, No. of 2005.

(ii) to an investigation or prosecution of a person or persons for an act constituting an unlawful activity, or may otherwise be of assistance in the enforcement of the Money laundering Act. No.5 of 2006 and the Convention on the Suppression of Terrorist Financing Act, No. 25 of 2005.

How to submit

Every institution must submit this form to the Director, FIU only through the Compliance Officer of the reporting institution designated under the FTRA. In urgent cases, the form should also be sent by fax:

Address: Director
Financial Intelligence Unit
Central Bank of Sri Lanka
30, Janadhipathi Mawatha
Colombo 1.
Fax. 94 11 2477692

FINANCIAL SUMMARY OVERVIEW:

- This is the snapshot of the account (account opening date, account closing date, if relevant) that may indicate the priority of the investigation.
- The snapshot of the account turnover may indicate the importance of the report too.

FINANCIAL SUMMARY DETAILS:

- As indicated above, the date of transaction in relation to the date of report and in relation to the date of receipt within the FIU can provide important inputs to the FIU.
- Counterparty information can help FIU to make comparative analysis with similar counterparties.
- Once again FIs should be encouraged to provide more reports.