POLICY FOR

PREVENTIONOF MONEY LAUNDERING
&
TERRORIST FINANCING

HAJJ FINANCE COMPANY LIMITED

Last Amended: March 2017

Preface

In response to the growing concern about money laundering and terrorist activities, government has enacted Money Laundering Prevention Act (MLPA), 2012 (repealing the MLPA, 2009) and Anti Terrorism Act (ATA), 2009 (as amended in 2012). Both the Acts have empowered Bangladesh Bank (BB) to perform the anchor role in combating ML & TF through issuing guidance and directives for reporting agencies including Financial Institutions (FIs), as defined in section 2(g) of MLPA, 2012. Accordingly as per circular no BFIU 04 dated 16.9.2012 HFCL and AML circular no 19/2008 dated 14.8.2008 the policy was formed and approved accordingly. Beside these as per the BFIU master circular no 12 dated 29.6.2015 and circular letter no 04/2015 dated 30.7.2015 have been is amended according to the Risk Assessment Report with the same circular.

HFCL Board of Directors in 33rd Board Meeting held on 30th December, 2012 approved the policy for Prevention of Money Laundering and Terrorist Financing in order to face the risk. Subsequently some amendments were incorporated vide approval from the Board of Directors meeting (38th Meeting held on 13th December 2013). As per the instruction clause no 1.1 of BFIU circular 12 dated 29.6.2015 some sections are amended in order to update the policy. Accordingly on 59th Board of Directors Meeting held on Thursday, March 9 2017 the policy was approved with the addition of the clauses.

These policies are designed to combating money laundering and terrorist financing and it is a dynamic approach, which can be modified and changed as per concern rules and regulation.

The prevention of money laundering and terrorist financing requires collective effort from all level of HFCL.

TABLE OF CONTENTS

CHAPTER 1: BACKGROUND

1.1 INTRODUCTION

Money Laundering is being employed by launderers worldwide to conceal the proceeds earned from criminal activities.

Money laundering has a major impact on a country‘s economy as a whole, impeding the social, economic, political, and cultural development of societies worldwide. Both money laundering and terrorist financing can weaken individual financial institution, and they are also a threat to a country‘s overall financial sector reputation. Combating money laundering and terrorist financing is, therefore, a key element in promoting a strong, sound and stable financial sector.

The process of money laundering and terrorist financing (ML/TF) is very dynamic and ever evolving. The money launderers and terrorist financers are inventing more and more complicated and sophisticated procedures and using new technology for money laundering and terrorist financing.

1.2 DEFINING MONEY LAUNDERING

Money Laundering is defined in Section 2 (v) of the Money Laundering Prevention Act 2012 as follows:

–**money laundering** means –

(i) knowingly moving, converting, or transferring proceeds of crime or property involved in an offence for the following purposes:-

1. concealing or disguising the illicit nature, source, location, ownership or control of the proceeds of crime; or
2. assisting any person involved in the commission of the predicate offence to evade the legal consequences of such offence;

(ii) smuggling money or property earned through legal or illegal means to a foreign country;

(iii) knowingly transferring or remitting the proceeds of crime to a foreign country or remitting or bringing them into Bangladesh from a foreign country with the intention of hiding or disguising its illegal source; or

(iv) concluding or attempting to conclude financial transactions in such a manner so as to reporting requirement under this Act may be avoided;

(v) converting or moving or transferring property with the intention to instigate or assist for committing a predicate offence;

(vi) acquiring, possessing or using any property, knowing that such property is the proceeds of a predicate offence;

(vii) performing such activities so as to the illegal source of the proceeds of crime may be concealed or disguised;

(viii) participating in, associating with, conspiring, attempting, abetting, instigate or counsel to commit any offences mentioned above;

1.3 STAGES OF MONEY LAUNDERING

Despite the variety of methods employed, money laundering is not a single act but a process accomplished in 3 basic stages which are as follows:

Placement - the physical disposal of the initial proceeds derived from illegal activity.

Layering - separating illicit proceeds from their source by creating complex layers offinancial transactions designed to disguise the audit trail and provide anonymity.

Integration - the provision of apparent legitimacy to wealth derived criminally. If thelayering process has succeeded, integration schemes place the laundered proceeds back into the economy in such a way that they re-enter the financial system appearing as normal business funds.

The three basic steps may occur as separate and distinct phases. These steps may comprise numerous transactions by the launderers that could alert a financial institution to criminal activity. They may also occur simultaneously or, more commonly, may overlap. How the basic steps are used depends on the available laundering mechanisms and the requirements of the criminal organizations.

1.4 DEFINING TERRORIST FINANCING

Terrorist financing can be simply defined as financial support, in any form, of terrorism or of those who encourage, plan, or engage in terrorism. The International Convention for the Suppression of the Financing of Terrorism (1999) under the United Nations defines TF in the following manner:

1. 'If any person commits an offense by any means, directly or indirectly, unlawfully and willingly, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out:

   a. An act which constitutes an offence within the scope of and as defined in one of the treaties listed in the link given below; or

   b. Any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking any active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing an act.

2. For an act to constitute an offense set forth in the preceding paragraph 1, it shall not be necessary that the funds were actually used to carry out an offense referred to in said paragraph 1, subparagraph (a) or (b)'[2].

According to the article 7 of the Anti Terrorism (Amendment) Act, 2012 of Bangladesh, financing of terrorism means:

Offences relating to financing terrorist activities.– (1) If any person or entity knowingly provides or expresses the intention to provide money, services, material support or any other property to another person or entity and where there are reasonable grounds to believe that the same have been used or may be used in full or partially for any purpose by a terrorist person, entity or group or organization, he or the said entity shall be deemed to have committed the offence of financing terrorist activities.

(2) If any person or entity knowingly receives money, services, material support or any other property from another person or entity and where there are reasonable grounds to believe that the same have been used or may be used in full of partially for any purpose by a terrorist person or entity or group or organization, he or the said entity shall be deemed to have committed the offence of financing terrorist activities.

(3) If any person or entity knowingly makes arrangement for money, services, material support or any other property for another person or entity where there are reasonable grounds to believe that the same have been used or may be used in full or partially for anypurpose by a terrorist person or entity or group or organization, he or the said entity shall be deemed to have committed the offence of financing terrorist activities.

(4) If any person or entity knowingly instigates another person or entity to provide or receive or make arrangement for money, services, material support or any other property in such a manner where there are reasonable grounds to believe that the same have been used or may be used in full or partially by a terrorist person or entity or group or organization for any purpose, he or the said entity shall be deemed to have committed the offence of financing terrorist activities.

1.5 THE LINK BETWEEN MONEY LAUNDERING AND TERRORIST FINANCING

The techniques used to launder money are essentially the same as those used to conceal the sources of, and uses for, terrorist financing. But funds used to support terrorism may originate from legitimate sources, criminal activities, or both. Nonetheless, disguising the source of terrorist financing, regardless of whether the source is of legitimate or illicit origin, is important. If the source can be concealed, it remains available for future terrorist financing activities. Similarly, it is important for terrorists to conceal the use of the funds so that the financing activity goes undetected.

As noted above, a significant difference between money laundering and terrorist financing is that the funds involved may originate from legitimate sources as well as criminal activities. Such legitimate sources may include donations or gifts of cash or other assets to organizations, such as foundations or charities that, in turn, are utilized to support terrorist activities or terrorist organizations.

1.6 THE BASEL COMMITTEE ON BANKING SUPERVISION

The Basel Committee on Banking Supervision (Basel Committee) was formed in 1974 by the central bank governors of the Group of Ten countries. Individual countries are represented by their central banks, or by the relevant authorities with formal responsibility for prudential supervision of banking where that authority is not the central bank. The committee has no formal international supervisory authority or force of law. Rather, it formulates broad supervisory standards and guidelines and recommends statements of best practices on a wide range of bank/financial institution supervisory issues. These standards and guidelines are adopted with the expectation that the appropriate authorities within each country will take all necessary steps to implement them through detailed measures, statutory, regulatory or otherwise, that best suit that country‘s national system. Three of the Basel Committee‘s supervisory standards and guidelines concern money laundering issues.

1.6.1 Statement of Principles on Money Laundering

In 1988, the Basel Committee issued its Statement on Prevention of Criminal Use of the Banking System for the Purpose of Money Laundering (Statement on Prevention). The Statement on Prevention outlines basic policies and procedures that managements of banks/FIs should undertake to assist in suppressing money laundering. There are essentially four principles contained in the Statement on Prevention:

Proper customer identification;

High ethical standards and compliance with laws;

Cooperation with law enforcement authorities; and

Policies and procedures to adhere to the statement.

1.6.2 Basel Core Principles for Banking

In 1997, the Basel Committee issued its Core Principles for Effective Banking Supervision (Core Principles), which provides a comprehensive blueprint for an effective bank supervisory system and covers a wide range of topics. Core Principle 15, one of the 25 Core Principles, deals with money laundering; it provides:

> *Banking supervisors must determine that banks have adequate policies, practices and procedures in place, including strict "know your customer" rules, that promote high ethical and professional standards in the financial sector and prevent the bank from being used; intentionally or unintentionally, by criminal elements.*

These ―know your customer‖ or ―KYC‖ policies and procedures are a crucial part of an effective institutional framework for every country.

In addition, the Basel Committee issued a –Core Principles Methodology‖ in 1999, which contains 11 specific criteria and five additional criteria to help assess the adequacy of KYC policies and procedures. These, additional criteria include specific reference to compliance with The Forty Recommendations.

1.6.3 Customer Due Diligence

In October, 2001, the Basel Committee issued an extensive paper on KYC principles, entitled Customer due diligence for banks/FIs (Customer Due Diligence). This paper was issued in response to noted deficiencies in KYC procedures on a world-wide basis. These KYC standards build upon and provide more specific information on the Statement on Prevention and Core Principle 15

CHAPTER 2: VULNERABILITIES OF FINANCIAL INSTITUTIONS

2.1 VULNERABILITIES OF PRODUCTS ANDSERVICES

2.1.1 Lease/Term Loan Finance

Fraud Company can take lease/term loan finance from a HFCL and repay the loan from illegal source, and thus bring illegal money in the formal financial system in absence of proper measures. The firm can also repay the loan amount even before maturity period if they are not asked about the sources of fund. In case of financial or capital lease, the asset purchased with HFCL‘s financing facility can be sold immediately after repayment of the loan through illegal money and sold proceeds can be shown as legal. So the money launderers and terrorist financer can use this financial instrument for placement and layering of their ill-gotten money.

2.1.2 Factoring:

In international factoring there is a provision that the two firms must be member of Factor Chain International or some association that can ensure the credit worthiness of the firms. In absence of this kind of private sector watchdog in the local factoring, the supplier and the buyer may ally together to legalize their proceeds of crime. Without conducting any bona fide transaction the supplier may get finance from HFCL and HFCL may get repayment from buyer. The management may focused on getting repayment without considering the sources fund which can be taken as an opportunity by the money launderer to place their ill-gotten money.

2.1.3 Private Placement of Equity/Securitization of Assets

The financing facilities to firms through private placement of equity and securitization of assets can be media of money laundering. HFCL sell those financial instruments to private investors who may take this as an opportunity to make their money legal. Later the money launderers can sell these instruments and bring their money in the formal financial system.

2.1.4 Personal Finance/Car Finance/Home Finance

Any person can take personal loan from HFCL and repay it by illegally earned money; thus he/she can launder money and bring it in the formal channel.

After taking home loan or car loan, money launderers can repay those with their illegally earned money, and later by selling that home/car, they can show the proceeds as legal money.

2.1.5 Consumer Loan

Consumer loan can take loan facilities from HFCL and repay that (in some cases before maturity) with illegally earned money. They even do so only to validate their money by even not utilizing the loan. This way they can bring the illegal money in the financial system.

2.1.6 Deposit Scheme

HFCL has different deposit products with at least a three months maturity period. However, the depositor can encash their deposit money prior to the maturity date foregoing profit income. This deposit product may be used as lucrative vehicle to place ill-gotten money in the financial system.

2.1.7 Loan Backed Money Laundering

In the ‗loan backed‘ money laundering method, a criminal provides an associate with a specific amount of illegitimate money. The associate then provides a ‗loan or mortgage‘ back to the money laundering for the same amount with all the necessary ‗loan or mortgage‘ documentation. This creates an illusion that the trafficker‘s funds are legitimate. The scheme is reinforced through ‗legislatively‘ scheduled payments made on the loan by the money launderer.

CHAPTER 3: COMPLIANCE REQUIREMENT

3.1 COMPLIANCE REQUIREMENTS UNDER THE LAWS

Compliance requirements for HFCL, as reporting organization, are based on Money Laundering Prevention Act (MLPA), 2012, Anti terrorism (Amendment) Act, 2012 and circulars or instructions issued by BFIU.

According to section 25 of MLPA, 2012 HFCLs' responsibilities to prevent money laundering are -

a) to maintain complete and correct information with regard to the identity of its customers during the operation of their accounts; *(For details please consult Chapter no 6)*

b) to preserve previous records of transactions of any customer's account for at least 5(five) years from the date of closure; *(For details please consult Chapter no 6)*

c) to provide with the information maintained under clauses (a) and (b) to Bangladesh Bank from time to time, on its demand;

d) if any suspicious transaction or attempt of such transaction as defined under clause (z)[3] of section 2 is observed, to report the matter as ‗suspicious transaction report' to the Bangladesh Bank immediately on its own accord. *(For details please consult Chapter no 7)*

According to section 16 of Anti Terrorism (Amendment) Act, 2012, HFCLs' responsibilities to combat financing of terrorism are -

(1) Every reporting agency shall take necessary measures, with appropriate caution and responsibility, to prevent and identify financial transactions which are connected to any offence under this Act and if any suspicious transaction is identified, the agency shall spontaneously report it to the Bangladesh Bank without any delay. (For details please consult Chapter no 7)

(2) The Board of Directors, or in the absence of the Board of Directors, the Managing Director, by whatever name called, of each reporting organization shall approve and issue directions regarding the duties of its officers, and shall ascertain whether the directions issued by Bangladesh Bank under section 15, which are applicable to the reporting agency, have been complied with or not.

3.2 COMPLIANCE REQUIREMENTS UNDER BFIU CIRCULARS

3.2.1. Policies for Prevention of Money Laundering and Terrorist Financing

In pursuance of section 16(2) of Anti terrorism (Amendment) Act, 2012, and Bangladesh Financial Intelligence Unit circular no 12 dated 29.6.2015 HFCL have incorporate policy manual to prevent money laundering and terrorist financing. This policy manual shall from time to time review and confirm the meticulous compliance of the circulars issued by Bangladesh Bank.

[3] section 2 (z) of MLPA, 2012–suspicious transaction‖ means such transactions –

(i) which deviates from usual transactions;

(ii) of which there is ground to suspect that,

(1) the property is the proceeds of an offence,

(2) it is financing to any terrorist activity, a terrorist group or an individual terrorist;

(iv) which is, for the purposes of this Act, any other transaction or attempt of transaction delineated in the instructions issued by Bangladesh bank from time to time.

3.2.2. **Commitment for Prevention of Money Laundering and Terrorist Financing**

Managing Director or CEO will declare a specific and effective commitment in order to prevent of Money Laundering and Terrorist Financing to all Department/Branch officer/staff on annually. He will specify the responsibility and duty of each staff regarding

the negligence of laws and instruction regarding AMCFT issue.

3.2.3. **Formation of Compliance Unit Head**

To implement the policy manual and compliance one high level officer as **Chief Anti-Money Laundering Compliance Officer (CAMLCO)**[5] in the Central Compliance Unit (CCU)[6] and one officer as Branch Anti-Money Laundering Compliance Officer (BAMALCO)[7] in each branch level is to be established. The details duties and responsibility are mentioned in the specific section.

3.2.4. **Customer Identification:**

It is mandatory to collect and verify the correct and complete identification of customers to prevent money laundering and terrorist financing and to keep the financial sector free from risks. As per AML circular, a customer is defined as:

- any person or institution maintaining an account of any type with HFCL or having business relationship with HFCL;
- the person or institution as true beneficial owner in whose favour the account is operated;
- the trustee, intermediary or true beneficial owner of the transaction of the accounts operated by the trust and professional intermediaries (such as lawyer/law firm, chartered accountant, etc) under the existing legal infrastructure;

3.2.4. To protect from risks of money laundering or/and terrorist financing by customers willful or unwilling activities, the Money Laundering Prevention Policy Manual shall clearly state how to conduct Customer Due Diligence at different stages such as:

- while establishing relationship with the customer;
- while conducting financial transaction with the existing customer;

3.2.4.1 To be sure about the customer's identity and underlying purpose of establishing relationship with HFCL, branch shall collect adequate information up to its satisfaction (*Satisfaction means satisfaction of the appropriate authority that necessary due diligence has been conducted considering the risks of the customers in the light of existing directions).*

3.2.4.2 If a person operates an account on behalf of the customer, the concerned branch official must satisfy itself that the person has due authorization to operate. Correct and complete information of the person, operating the account, is to be collected.

3.2.4.3 Legal status and accuracy of information of the operators are to be ascertained in case of the accounts operated by trustee and professional intermediaries (such as lawyers/law firm, chartered accountants, etc).

3.2.4.4 While establishing and maintaining business relationship and conducting financial transaction with a person (including legal representative, financial institution or any other institution) of the countries and territories that do not meet international standard in combating money laundering (such as the countries and territories listed as high risk country in FATF's public statements) enhanced due diligence shall have to be ensured.

3.2.4.5 The identity of the beneficial owner of the account shall have to be confirmed on the basis of the information obtained from reliable sources up to the satisfaction of the institution. Moreover, FIs have to do the followings:

- Complete and correct information of identity of the persons besides the customer, shall have to be collected and preserved if a customer operate an account on behalf of another person in his/her own name.

- The controller or the owner of the customer shall have to be identified.
- Complete and correct information of identity of the beneficial owners shall have to be collected and preserved. For the purpose of this subsection, a person will be treated as a beneficial owner if:
  a) he has controlling share of a company or/and
  b) hold 20% or more shares of a company.

3.2.5. Politically exposed Persons (PEPs)

While opening and/or operating account of Politically Exposed Persons (PEPs)[9] enhanced due diligence shall have to be exercised.

Following instructions shall have to be followed to ensure Enhanced Due Diligence:

- identify risks associated with the accounts opening and operating of PEPs;
- take reasonable measures to establish the source of wealth and source of funds;
- ongoing monitoring of the transactions have to be conducted; and
- the branch should observe all formalities as detailed in Guidelines for Foreign Exchange Transactions while opening accounts of non-residents;

All instructions as detailed for PEPs shall be equally applicable if business relationship is established with family members and close associates of these persons who may pose reputational risk.

The above instructions shall also be applicable to customers or beneficial owners who become PEPs after business relationship have been established.

3.2.5 **Appointment and Training**

3.2.6.1 Employee Screening: One of the major purposes of combating money laundering and terrorist financing activities is to protect HFCL from risks arising out of money laundering and terrorist financing. To meet this objective, human resources department shall have to undertake proper screening mechanism in their different appointment procedures so that they do not face money laundering and terrorist financing risks by any staff.

3.2.6.2 Training for the officials: To ensure proper compliance of ML/TF activities management of HFCL shall arrange suitable training for their officials periodically.

3.2.6.3 Education and training for customers: Official of HFCL shall respond tocustomers on different matters including KYC. Marketing Department or Liability Department shall time to time distribute leaflets among customers to make them aware about money laundering and terrorist financing and will arrange to stick posters in every branch at a visible place.

3.3 SUSPICIOUS TRANSACTION REPORTING (STR)

According to the provision of section 25 (1) (d) of MLPA, 2012, the concern official have to report to CAMLCO through BAMLCO proactively and immediately, facts on suspicious, unusual or doubtful transactions likely to be related to money laundering. According to section 15(a) of Anti terrorism (Amendment) Act, 2012 BB has the power to call STR through CAMLCO related to financing of terrorism (For details please consult Chapter 7).

3.4 TARGETED FINANCIAL SANCTIONS:

United Nations Security Council Resolution 1267 and 1373 have been adopted under Article VII of UNSCR charter, which means these resolutions are obligatory for every jurisdiction. Branch is to take necessary action on UNSCR 1267 and 1373 (targeted financial sanctions).

3.5 SUPERVISORY POWER OF BANGLADESH BANK

According to the provision laid down in the section 23 of MLPA, 2012 and section 15 of Anti terrorism (Amendment) Act, 2012, Bangladesh Bank is the core implementing agency. The major supervisory powers are:

[9] PEPs means –Individuals who are or have been entrusted with prominent public functions in a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials‖.

Under MLPA, 2012, Bangladesh Bank shall have the following powers and responsibilities to prevent money laundering and to resist any such activities:

a) to analyze or review information related to cash transactions and suspicious transactions received from any reporting organization and to collect additional information relating thereto for the purpose of analyzing or reviewing from the reporting organizations and maintain data on the same and, as the case may be, provide with the said information to the relevant law enforcement agencies for taking necessary actions;

b) ask for any information or obtain a report from reporting organizations with regard to any transaction in which there are reasonable grounds to believe that the transaction is involved in money laundering or a predicate offence;

c) issue an order to any reporting organization to suspend or freeze transactions of any account for a period not exceeding 30 (thirty) days if there are reasonable grounds to suspect that any money or property has been deposited into the account by committing any offence;

   Provided that such order may be extended for additional period of a maximum of 6 (six) months by 30 (thirty) days, if it appears necessary to find out correct information relating to transactions of the account;

d) issue, from time to time, any direction necessary for the prevention of money laundering to the reporting organizations;

e) monitor whether the reporting organizations have properly submitted information and reports requested by Bangladesh Bank and whether they have duly complied with the directions issued by it, and where necessary, carry out on-site inspections of the reporting organizations to ascertain the same;

f) arrange meetings and seminars including training for the officers and staff of any organization or institution, including the reporting organizations, considered necessary for the purpose of ensuring proper implementation of this Act by Bangladesh Bank;

g) carry out any other functions necessary for the purposes of this Act.

The power and responsibilities of Bangladesh Bank under section 15(1) of Anti Terrorism (Amendment) Act, 2012 are as follows:

The Bangladesh Bank shall have the power and authority to take necessary measures to prevent and detect transaction intended to commit offence under ATA through any banking channel, and for that matter BB is empowered and authorized to -

- Call for STRs from financial institutions and keep such report confidential if law does not allow disclosure;
- Compile and preserve all statistics and records;
- Create and maintain a database of all STRs;
- Analyze the STRs;
- Issue order in writing to suspend a transaction for a period of 30 days where it has reasonable grounds to suspect that the transaction involves connection with terrorist acts, and extend the order to maximum 180 days.
- Monitor and observe the activities of financial activities;
- Issue instructions to take preventive measures against terrorist financing activities.

- Inspect for the purpose of detection of suspicious transactions connected with terrorist financing; and
- Provide training to staff and officers for the purpose of detection and prevention of suspicious transactions as may be connected with terrorist financing.

- **It is to be noted that no law enforcement authority shall have any access to the documents or files of a financial institution without approval from the Managing Director of HFCL or from Bangladesh Bank.**

3.6 PENALTIES UNDER MLPA:

According to section 25 (2) of MLPA, 2012, violating the directions mentioned in sub-section (1) of section 25 of MLPA, 2012, Bangladesh Bank may-

(a) impose a fine of at least taka 50 (fifty) thousand but not exceeding taka 25 (twenty five) lacs; and (b) in addition to the fine mentioned in clause (a), cancel the license or the authorization for carrying out commercial activities or any of its branches, service centers, booths or agents, or as the case may be, shall inform the registration or licensing authority about the fact so as to the relevant authority may take appropriate measures against HFCL.

In addition to the above mentioned provisions there are some new provisions of penalties in the section 23 of MLPA, 2012. These are:

(3) Failure to provide the requested information timely under this section, Bangladesh Bank may impose a fine which may extend to a maximum of Taka 5 (five) lacs at the rate of Taka 10 (ten) thousand per day and if it is fined more than 3(three) times in 1(one) financial year, Bangladesh Bank may suspend the registration or license of the organization or any of its branches, service centers, booths or agents for the purpose of closing its operation within Bangladesh or, as the case may be, shall inform the registration or licensing authority about the fact so as to the relevant authority may take appropriate measures.

If provides with false information or statement requested under this section, Bangladesh Bank may impose a fine not less than Taka 20 (twenty) thousand but not exceeding Taka 5 (five) lacs and if fined more than 3(three) times in 1(one) financial year, Bangladesh Bank may suspend the registration or license of the organization or any of its branches, service centers, booths or agents for the purpose of closing its operation within Bangladesh or, as the case may be, shall inform the registration or licensing authority about the fact so as to the relevant authority may take appropriate measures.

(4) If fails to comply with any instruction given by Bangladesh Bank under this Act, Bangladesh Bank may impose a fine which may extend to a maximum of Taka 5 (five) lacs at the rate of Taka 10 (ten) thousand per day for each of such non compliance and if it is fined more than 3(three) times in 1(one) financial year, Bangladesh Bank may suspend the registration or license any branches, service centers, booths or agents for the purpose of closing its operation within Bangladesh or, as the case may be, shall inform the registration or licensing authority about the fact so as to the relevant authority may take appropriate measures.

(5) If it fails to comply with any order for freezing or suspension of transaction issued by Bangladesh Bank under clause (c) of sub-section 23(1) of MLPA, 2012, Bangladesh Bank may impose a fine not less than the balance held on that account but not more than twice of the balance held at the time of issuing the order.

(7) If any person or entity fails to pay any fine imposed by Bangladesh Bank under sections 23 and 25 of this Act, Bangladesh Bank may recover the fine from accounts maintained in the name of the relevant person, entity or reporting organization in any bank or financial institution or Bangladesh Bank, and in this regard if any amount of the fine remains unrealized, Bangladesh

Bank may, if necessary, make an application before the court for recovery and the court may pass such order as it deems fit.

(8) If any fine is imposed under sub-sections 23 (3), (4), (5) and (6), Bangladesh Bank may also impose a fine not less than Taka 10 (ten) thousand but not exceeding taka 5 (five) lacs on the responsible owner, directors, officers and staff or persons employed on contractual basis of HFCL and, where necessary, may direct HFCL to take necessary administrative actions

.

3.7 PENALTIES UNDER ATA:

The provision laid down in section 16 (3) of Anti Terrorism (Amendment) Act, 2012, if reporting authority fails to comply with the directions issued by Bangladesh Bank under section 15 or knowingly provides any wrong or false information or statement, the said reporting agency shall be liable to pay a fine determined and directed by Bangladesh Bank not exceeding Taka 10 (ten) lacs and Bangladesh Bank may suspend the registration or license with intent to stop operation of the said agency or any of its branches, service centers, booths or agents within Bangladesh or, as the case may be, shall inform the registering or licensing authority about the subject matter to take appropriate action against the agency. According to section 16 (4) if any reporting agency fails to pay or does not pay any fine imposed by Bangladesh Bank according to sub-section 16 (3) of ATA, Bangladesh Bank may recover the amount from the reporting agency by debiting its accounts maintained in any bank or Bangladesh Bank and in case of any unrealized or unpaid amount, Bangladesh Bank may, if necessary, apply before the concerned court for recovery.

3.8 SELF ASSESSMENT

As per Master Circular clause no 8.1 each branch will assess its Money Laundering and Terrorist Financing prevention activities under Self Assessment procedure under a prescribed checklist half yearly basis. This procedure enables management to identify areas of risk or to assess the need for additional control mechanisms. The self-assessment will conclude with a report documenting the work performed, how it was controlled/ supervised and the resulting findings, conclusions and recommendations.

After self assessment a report will be prepared to assess the action and initiative required for effective compliance. Before finalize the report a meeting headed by branch manager. Branch manager will discuss on the draft report and if any problem identified in the draft report can be solved at branch level after that report will be finalized including the decision dully recorded in the report.

Subsequently the progress of decisions will be discussed in quarterly Prevention of Money Laundering and Terrorist Financing meeting at branch level. The Branch Evaluation Report will be sent to Internal Audit Department and Central Compliance Unit within **15(fifteen) days** including the action taken or action to be taken and recommendation.

The following criteria can be assessed in the Self Assessment Procedure:

- The percentage of officers/employees that received official training on AML/CFT;
- The awareness of the officers/employees about the internal AML/CFT policies, procedures and programs, and Bangladesh Bank‘s instructions and guidelines;
- The arrangement of AML/CFT related meeting on regular interval;
- The effectiveness of the customer identification during opening an individual, corporate and other account;

- The risk categorization of customers by the branch;
- Regular update of customer profile upon reassessment;
- The monitoring of customers' transactions with their declared TP after categorizing the customers based on risk or transactions over specific limit;
- Identification of Suspicious Transaction Reports (STRs);
- The maintenance of a separate file containing MLPA, Circulars, Training Records, Reports and other AML related documents and distribution of those among all employees;
- The measures taken by the branch during opening of account of PEPs;
- Consideration of UN Sanction List while conducting any business.
- The compliance with AML/CFT weaknesses/irregularities, as the bank's Head Office and Bangladesh Bank's inspection report mentioned.

3.9 INDEPENDENT TESTING PROCEDURE

As per instruction clause no 8.2 of master circular after verifying the Branch Evaluation Report if any risky issue found by Internal Audit Department, Internal Audit Department will immediately arrange a inspect of the concern branch and subsequently inform the Central Compliance Unit.

Internal Audit Department, at the time for preparing the branch inspection/audit schedule within their own policy and regular annual programme they will perform the Independent Testing Procedure under a set checklist and they will also rate the branch as well as the branch report.

Internal Audit Department will provide the report along with the branch rating report to the Central Compliance Unit.

The test will cover the following areas:

- Branch Compliance Unit/BAMLCO
- Knowledge of officers/employees on AML/CFT issues
- Customer Identification (KYC) process
- Branch's receipt of customer's expected transaction profile and monitoring
- Process and action to identify Suspicious Transaction Reports (STRs)
- Regular submission of reports to CCU
- Proper record keeping
- Overall AML related activities by the branch

The tests include interviews with employees handling transactions and interviews with their supervisors to determine their knowledge and compliance with the branch's anti-money laundering procedures.

- sampling of large transactions followed by a review of transaction record retention forms and suspicious transaction referral forms;
- test of the validity and reasonableness of any exemption granted by the branch/head office; and
- test of the record keeping system according to the provisions of the laws. Any deficiencies should be identified and reported to senior management together with a request for a response indicating corrective action taken or to be taken and a deadline.

CHAPTER 4: COMPLIANCE PROGRAM

In order to maintain an effective AML/CFT program it should includes at the followings:

- Development of internal policies, procedures and controls;
- Appointment of an AML/CFT Compliance Officer;
- Ongoing employee training programs; and
- Independent audit function including internal and external audit function to test the programs.

The compliance program should be documented, approved by the Board of Directors and communicated to all levels of the organization. In developing an AML/CFT compliance program, attention should be paid to the size and range of activities, complexity of operations, and the nature and degree of ML and/or TF risks associated with FIs.

4.1 DEVELOPMENT OF INTERNAL POLICIES, PROCEDURES AND CONTROLS

4.1.1 Internal Policy

HFCL will develop, administer, and maintain its own AML/CFT policy that ensures and monitors compliance with the laws, including record keeping and reporting requirements. Such a compliance policy must be written, approved by the board of directors, and noted as such in the board meeting minutes.

The written AML/CFT compliance policy at a minimum should establish clear responsibilities and accountabilities within our organizations to ensure that policies, procedures, and controls are introduced and maintained which can deter criminals from using their facilities for money laundering and the financing of terrorist activities, thus ensuring that they comply with their obligations under the Act.

The policies will be tailored to the institution and would have to be based upon an assessment of the money laundering and terrorist financing risks, taking into account the financial institution's business structure and factors such as its size, location, activities, methods of payment, and risks or vulnerabilities to money laundering and terrorist financing.

It will include standards and procedures to comply with applicable laws and regulations to reduce the prospect of criminal abuse. The procedures should address its Know Your Customer (KYC) policy and identification procedures before opening new accounts, monitoring existing accounts for unusual or suspicious activities, information flows, reporting suspicious transaction, hiring and training employees and a separate audit or internal control function to regularly test the program‘s effectiveness.

It will also include a description of the roles the AML/CFT Compliance Officer(s)/Unit and other appropriate personnel will play in monitoring compliance and effectiveness of AML/CFT policies and procedures.

It will develop and implement screening programs to ensure high standards when hiring employees. Implement standards for employees who consistently fail to perform in accordance with an AML/CFT framework.

It will incorporate AML/CFT compliance into job descriptions and performance evaluations of appropriate personnel.

It will have the arrangements for program continuity despite changes in management or employee composition or structure.

The AML/CFT policies will be reviewed regularly and updated as necessary and at least annually based on any legal/regulatory or business/operational changes, such as additions or amendments to existing AML/CFT related rules and regulations or business.

In addition the policy will emphasize the responsibility of every employee to protect the institution from exploitation by money launderers and terrorist financiers, and will set forth the consequence of non-compliance with the applicable laws and the institution's policy, including the criminal, civil and disciplinary penalties and reputational harm that could ensue from any association with money laundering and terrorist financing activity.

The most important element of a successful AML/CFT program is the commitment of senior management, including the chief executive officer and the board of directors, to the development and enforcement of the AML/CFT programs which can deter criminals from using their facilities for money laundering and terrorist financing, thus ensuring that they comply with their obligations under the laws.

4.1.1.1 Components of Policy

The statement of compliance policy will at a minimum include:

- A statement that all employees are required to comply with applicable laws and regulations and corporate ethical standards.
- A statement that all activities carried out by the HFCL must comply with applicable governing laws and regulations.
- A statement that compliance with rules and regulations is the responsibility of each individual of HFCL in the normal course of their assignments. It is the responsibility of the individual to become familiar with the rules and regulations that relate to his or her assignment. Ignorance of the rules and regulations cannot be an excuse for non-compliance.
- A statement that should direct staff to a compliance officer or other knowledgeable individuals when there is a question regarding compliance matters.
- A statement that employees will be held accountable for carrying out their compliance responsibilities.

4.1.1.2 Communicating the Policy

As part of its AML/CFT policy, it is be communicated clearly to all employees of HFCL on annual basis through a statement from the chief executive officer that clearly sets forth its policy against money laundering and any activity which facilitates money laundering or the funding of terrorist or criminal activities. Such a statement evidence the strong commitment of the institution and its senior management to comply with all laws and regulations designed to combat money laundering and terrorist financing.

4.1.2 Procedures

The standard operating procedures are often designed at a lower level in the organization and modified as needed to reflect the changes in products, personnel and promotions, and other day to day operating procedures. It will be more detailed than policies. Standard operating procedures translate policy into an acceptable and working practice. In addition to policies and procedures, there should also be a process to support and facilitate effective implementation of procedures and that should be reviewed and updated regularly.

4.1.3 Internal Control Mechanism

The compliance program also relies on the variety of internal controls, including management report, built-in safeguards and exception report that keep the program working. As per FATF recommendation 18 requires that every financial institutions have an internal control program.

The following elements should be included in the operational controls of any policy:

- Statement of responsibility for compliance with policy;
- Customer due diligence;
  - Customer identification/verification
  - Additional know your customer information
  - High risk customers
  - Non face to face business (if applicable)
  - Handling of politically exposed persons
- Monitoring for suspicious transaction/activity;
- Cooperation with the authorities;
- Record keeping ;
- Screening of transactions and customers;
- Training and awareness;
- Adoption of risk management practices and use of a risk-based approach.

4.2 ESTABLISH OF CENTRAL COMPLIANCE UNIT (CCU)

In order to face the risk of Money Laundering and Terrorist Financing and prevent the Money Laundering and Terrorist Financing a Central Compliance Unit under a leadership of a high official will be formed. This unit will be under supervision of Managing Director. The team leader will be designated as Chief Ani Money Laundering Compliance Officer (CAMLCO). He will have sufficient authority to implement and enforce corporate-wide AML/CFT policies, procedures and measures. The CAMLCO will directly report to the Managing Director. The CAMLCO will also be responsible to coordinate and monitor day to day compliance with applicable AML/CFT related laws, rules and regulations as well as with its internal policies, practices, procedures and controls.

4.2.1 Position of CAMLCO

The Chief AML/CFT Compliance Officer will be the head of CCU. The designated CAMLCO, directly or through CCU, should be a central point of contact for communicating with the regulatory and/or investigation agencies regarding issues related to financial institution's AML/CFT program. The position of the CAMLCO cannot be lower than the third rank in seniority in organizational hierarchy. A Deputy Chief Anti Money Laundering Compliance Officer-DCAMLCO can be designated to help CAMLCO.

4.2.2 Qualification and experience

The CAMLCO should have a working knowledge of the diverse financial products offered by the financial institutions. The person could have obtained relevant financial institutional and compliance experience as an internal auditor or regulatory examiner, with exposure to different financial institutional products and businesses. Product and financial institutional knowledge could be obtained from being an external or internal auditor, or as an experienced operational staff. The Chief AML/CFT Compliance Officer should have a minimum of seven years of working experience, with a minimum of three years at a managerial/administrative level. The Deputy Chief Anti Money Laundering Compliance Officer should have a minimum 5(five) years of experience.

4.2.3 Responsibilities:

Depending on the scale and nature of the financial institution the designated Chief and Deputy Chief AML/CFT Compliance Officer may choose to delegate duties or rely on suitably qualified staff for their practical performance whilst remaining responsible and accountable for the operation of the designated functions. The major responsibilities of a CAMLCO and Deputy CAMLCO are as follows:

1. To monitor, review and coordinate application and enforcement of the financial institution's compliance policies including AML/CFT Compliance Policy. This will include - an AML/CFT risk assessment, practices, procedures and controls for account opening, KYC procedures and ongoing account/transaction monitoring for detecting suspicious transaction/account activity, and a written AML/CFT training plan.
2. To monitor changes of laws/regulations and directives of Bangladesh Bank and revise its internal policies accordingly;
3. To respond to compliance questions and concerns of the staff and advise regional offices/branches/units and assist in providing solutions to potential issues involving compliance and risk;
4. To ensure that the financial institution's AML/CFT policy is complete and up-to-date, to maintain ongoing awareness of new and changing business activities and products and to identify potential compliance issues that should be considered by the financial institution;
5. To develop the compliance knowledge of all staff, especially the compliance personnel and conduct training courses in the institution in this regard;
6. To develop and maintain ongoing relationships with regulatory authorities, external and internal auditors, regional/branch/unit heads and compliance resources to assist in early identification of compliance issues;
7. To assist in review of control procedures in the financial institution to ensure legal and regulatory compliance and in the development of adequate and sufficient testing procedures to prevent and detect compliance lapses;
8. To monitor the business through self-testing for AML/CFT compliance and take any required corrective action;
9. To manage the STR/SAR process:
    - reviewing transactions referred by divisional, regional, branch or unit compliance officers as suspicious;
    - reviewing the transaction monitoring reports (directly or together with account management personnel);
    - ensuring that internal Suspicious Activity Reports (SARs):
        - are prepared when appropriate;
        - reflect the uniform standard for ―suspicious activity involving possible money laundering or terrorist financing‖ established in its policy;
        - are accompanied by documentation of the branch's decision to retain or terminate the account as required under its policy;
        - are advised to other branches of the institution who are known to have a relationship with the customer;
        - are reported to the Managing Director and the Board of Directors of the institution when the suspicious activity is judged to represent significant risk to the institution, including reputation risk.
    - ensuring that a documented plan of corrective action, appropriate for the seriousness of the suspicious activity, be prepared and approved by the branch manager;
    - maintaining a review and follow up process to ensure that planned corrective action, including possible termination of an account, be taken in a timely manner;
    - managing the process for reporting suspicious activity to BFIU after appropriate internal consultation;
10. 10. Central Compliance Unit will prepare a half yearly report regarding the initiative taken, progress and recommendation related with prevention of Money Laundering and Terrorist

Activities (Jan-June, Jul-Dec) to Managing Director. This report will be placed to the Board of Directors meeting with the instruction and comments of Managing Director and this report will be sent to BFIU within two month after completion of half year.

11. The Central Compliance Unit will designate the Branch Anti Money Laundering Officer (BAMLCO) with responsibility assigned to him.
12. The Central Compliance Unit will give instruction to the branches regarding Prevention of Money Laundering and Terrorist Financing, transaction analysis procedure, Internal Control, policy and procedure.
13. The Central Compliance Unit will inform BFIU if any information regarding the Terrorist Financing for Money Laundering, whether any news is published to any media and submit STR in case applicable.

4.3 BRANCH ANTI-MONEY LAUNDERING COMPLIANCE OFFICER

HFCL will appoint Branch Anti-Money Laundering Compliance Officer (BAMLCO) at each branch who will establish the existing laws, rules, BFIU instruction and HFCL policy regarding prevention of Money Laundering and Terrorist Financing. BAMLCO will be the second man of a branch and have a minimum three year experience in related field. The responsibilities of a BAMLCO are as follows:

- Branch Anti Money Laundering Compliance Officer will sit for discussion in every three month interval with other important branch officers and will discuss the following issue under AM/CFT circular, laws and policy.

I) Customer Information (KYC)
II) Transaction Monitoring
III) Suspicious Transaction and Suspicious Activities identification and reporting
IV) Record Keeping
V) Training of Staff
VI) Reporting Self Assessment Report to CCU

4.4 RESPONSIBILITIES OF OTHER EMPLOYEES

The table below details the individual responsibilities of the employees of HFCL:-

Function	Role / Responsibilities
Staff Responsible for account opening	• Perform due diligence on prospective clients prior opening an account • Be diligent regarding the identification (s) of account • holder and the transactions relating to the account • Ensure all required documentation is completed satisfactorily • Complete the KYC Profile for the new customer • Ongoing monitoring of customers KYC profile and transaction activity • Escalate any suspicion to the Supervisor, Branch Manager and BAMLCO
Customer Service Officer	• Support the Account Officer in any of the above roles • Perform the Account Officer roles in their absence
Operations Staff	• Ensure that all control points are completed prior to transaction monitoring • Be diligence on transaction trends for clients • Update customer transaction profiles in the ledger/system
Branch Manager (Unit Head)	• Ensure that the program is effective within the branch/unit • First point of contact for any issues

Function	Role / Responsibilities
Risk Management/Credit Officer/ Internal Control Officer	• Perform Risk Assessment for the Business • Perform periodic Quality Assurance on the program in the unit • Communicate updates in laws and internal policies
Operations & Technology Manager	• Ensures that the required reports and systems are in place to maintain an effective program
Controller of Branches	• Overall responsibility to ensure that the branches have an program in place and that it is working effectively
Managing Director	• Overall responsibility to ensure that the Business has an AML program in place and it is working effectively

4.5 EMPLOYEE TRAINING AND AWARENESS PROGRAM

The AML/CFT compliance program should include an ongoing employee training program. The importance of a successful training and awareness program cannot be overstated. Employees in different business functions need to understand how the financial institution's policy, procedures, and controls affect them in their day to day activities. HFCL shall arrange suitable training for their officials to ensure proper compliance of money laundering and terrorist financing prevention activities.

4.5.1 The Need for Staff Awareness

The effectiveness of the procedures and recommendations contained in these Guidance Notes must depend on the extent to which staff in institution appreciates the seriousness of the background against which the legislation has been enacted. Staff must be aware of their own personal statutory obligations and that they can be personally liable for failure to report information in accordance with internal procedures. All staff must be trained to co-operate fully and to provide a prompt report of any suspicious transactions/activities.

It is, therefore, important that comprehensive measuresshould be introduced to ensure that all staff and contractually appointed agents are fully aware of their responsibilities.

4.5.2 Education and Training Programs

All relevant staff should be educated in the process of the **–Know Your Customer‖** requirements for money laundering and terrorist financing prevention purposes. The training in this respect should cover not only the need to know the true identity of the customer but also, where a business relationship is being established, the need to know enough about the type of business activities expected in relation to that customer at the outset to know what might constitute suspicious activity at a future date. Relevant staff should be alert to any change in the pattern of a customer's transactions or circumstances that might constitute criminal activity.

Although Directors and Senior Managers may not be involved in the day-to-day procedures, it is important that they understand the statutory duties placed on them, their staff and the institution itself. Some sorts of high-level general awareness raising training are, therefore, also suggested.

4.5.3 General Training

A general training program should include the following:

- General information on the risks of money laundering and terrorist financing schemes, methodologies, and typologies;
- Legal framework, how AML/CFT related laws apply to FIs and their employees;
- Institution‘s policies and systems with regard to customer identification and verification, due diligence , monitoring;
- How to react when faced with a suspicious client or transaction;
- How to respond to customers who want to circumvent reporting requirements;
- Stressing the importance of not tipping off clients;
- Suspicious transaction reporting requirements and processes;
- Duties and accountabilities of employees;

The person responsible for designing the training must identify which, if any, of these topics relate to the target audience. Effective training should present real life money laundering schemes, preferably cases that have occurred at the institution or at similar institutions, including, where applicable, how the pattern of activity was first detected and its ultimate impact on the institution.

4.5.4 Job Specific Training

The nature of responsibilities/activities performed by the staff of a financial institution is different from one another. So their training on AML/CFT issues should also be different for each category. Job specific AML/CFT trainings are discussed below:

4.5.4.1 New Employees

A general appreciation of the background to money laundering and terrorist financing, and the subsequent need for reporting any suspicious transactions should be provided to all new employees who are likely to be dealing with customers or their transactions, irrespective of the level of seniority. They should be made aware of the importance placed on the reporting of suspicions by the organization, that there is a legal requirement to report, and that there is a personal statutory obligation to do so.

4.5.4.2 Customer Service/Relationship Managers

Members of staff who are dealing directly with the public are the first point of contact with potential money launderers and terrorist financiers and their efforts are vital to the organization's strategy in the fight against money laundering and terrorist financing. They must be made aware of their legal responsibilities and should be made aware of the organization's reporting system for such transactions. Training should be provided on factors that may give rise to suspicions and on the procedures to be adopted when a transaction is deemed to be suspicious.

It is vital that **'front-line'** staffs are made aware of the organization's policy for dealing with non-regular (walk-in) customers particularly where large transactions are involved, and the need for extra vigilance in these cases.

4.5.4.3 Processing (Back Office) Staff

The staffs, who receive completed Account Opening, FDR application forms and cheques for deposit into customer‘s account or other investments must receive appropriate training in the processing and verification procedures. The staffs, who are in a position to deal with account opening, or to accept new customers, must receive the training given to relationship managers and other front office staff above. In addition, the need to verify the identity of the customer must be understood, and training should be given in the organization's account opening and customer/client verification procedures. Such staff should be aware that the offer of suspicious funds or the request to undertake a suspicious transaction may need to be reported to the AML/CFT Compliance Officer (or alternatively a line supervisor) whether or not the funds are accepted or the transactions proceeded with and must know what procedures to follow in these circumstances.

4.5.4.4 Credit Officers:

Training should reflect an understanding of the credit function. Judgments about collateral and credit require awareness and vigilance toward possible laundering and funding terrorists. Indirect lending programs and lease financing also call for KYC efforts and sensitivity to laundering risks.

4.5.4.5 Audit and compliance staff

These are the people charged with overseeing, monitoring and testing AML/CFT controls, and they should be trained about changes in regulation, money laundering and terrorist financing methods and enforcement, and their impact on the institution.

4.5.4.6 Senior Management/Operations Supervisors and Managers

A higher level of instruction covering all aspects of money laundering and terrorist financing prevention procedures should be provided to those with the responsibility for supervising or managing staff. This will include the offences and penalties arising from the laws for non-reporting and for assisting money launderers and terrorist financers; internal reporting procedures and the requirements for verification of identity and the retention of records.

4.5.4.7 Senior Management and Board of Directors

Money laundering and terrorist financing issues and dangers should be regularly and thoroughly communicated to the board. It is important that the compliance department has strong board support, and one way to ensure that is to keep board members aware of the reputational risk that money laundering and terrorist financing poses to the institution. Major AML/CFT compliance related circulars/circular letters issued by BB should be placed to the board to bring it to the notice of the board members.

4.5.4.8 AML/CFT Compliance Officer

The AML/CFT Compliance Officer should receive in depth training on all aspects of the Money Laundering and Terrorist Financing Prevention Legislation, Bangladesh Bank directives and internal policies.

In addition, the AML/CFT Compliance Officer will require extensive instructions on the validation and reporting of suspicious transactions and on the feedback arrangements, and on new trends and patterns of criminal activity.

4.5.5 Training Procedures

The trainers can take the following steps to develop an effective training program:

- Identify the issues that must be communicated and decide how best to do this e.g. sometimes, e-learning can effectively do the job, sometimes classroom training is the best option.
- Identify the audience by functional area as well as level of employee/management. This should be accompanied by a quick ―why are they hereassessment. New hires should receive training different from that given to veteran employees.
- Determine the needs that are being addressed; e.g. uncovered issues by audits or examinations, created by changes to systems, products or regulations.
- Determine who can best develop and present the training program.
- Create a course abstract or curriculum that addresses course goals, objectives and desired results. Be sure to identify who the audience should be and how the material will be presented.
- Establish a training calendar that identifies the topics and frequency of each course.
- Course evaluation shall be done to evaluate how well the message is received; copies of the answer

key should be made available. Similarly, in case of a case study used to illustrate a point, provide detailed discussion of the preferred course of action.

- Track Attendance by asking the attendees to sign in. Employee who shall remain absent without any reason may warrant disciplinary action and comments in employee‘s personal file.

4.5.6 Refresher Training

In addition to the above compliance requirements, training may have to be tailored to the needs of specialized areas of the institution‘s business. It will also be necessary to keep the content of training programs under review and to make arrangements for refresher training at regular intervals i.e. at least annually to ensure that staff does not forget their responsibilities. The Human Resources Department may provide such training on an annual basis; or choose a shorter or longer period or wish to take a more flexible approach to reflect individual circumstances, possibly in conjunction with compliance monitoring.

Training should be conducted ongoing basis, incorporating trends and developments in an institution‘s business risk profile, as well as changes in the legislation. Training on new money laundering and terrorist financing schemes and typologies are of the utmost importance when reviewing policies and controls and designing monitoring mechanisms for suspicions activity.

4.6 INDEPENDENT AUDIT FUNCTION

4.6.1 Why the audit function is necessary

To ensure the effectiveness of the AML/CFT program, financial institution should assess the program regularly and look for new risk factors. It should covered by laws establish and maintain policies, procedures and controls which should include an appropriate compliance function and an audit function.

4.6.2 Why the audit function must be independent

The audit must be independent (i.e. performed by people not involved with the AML/CFT compliance staff). Audit is a kind of assessment of checking of a planned activity. Only those will check or examine the institution who do not have any stake in it. To ensure objective assessment it is important to engage an independent body to do audit.

4.6.3 Whom they report

The individuals conducting the audit should report directly to the Managing Director.

4.6.4 The ways of performing audit function

Audit function shall be done by the internal audit. At the same time external auditors appointed by the HFCL to conduct annual audit shall also review the adequacy of AML/CFT program during their audit.

4.7.5 Internal audit

Internal auditors should be well resourced and enjoy a degree of independence within the organization. Those performing the independent testing must be sufficiently qualified to ensure that their findings and conclusions are reliable. The responsibilities of internal auditors are:

- Address the adequacy of AML/CFT risk assessment.
- Examine/attest the overall integrity and effectiveness of the management systems and the control environment.
- Examine the adequacy of Customer Due Diligence (CDD) policies, procedures and processes, and whether they comply with internal requirements.
- Determine personnel adherence to the financial institution‘s AML/CFT policies, procedures and

processes.

- Perform appropriate transaction testing with particular emphasis on high risk operations (products, service, customers and geographic locations).
- Assess the adequacy of the FI‘s processes for identifying and reporting suspicious activity.
- Communicate the findings to the board and/or senior management in a timely manner.
- Recommend corrective action for deficiencies.
- Track previously identified deficiencies and ensure that management corrects them.
- Assess training adequacy, including its comprehensiveness, accuracy of materials, training schedule and attendance tracking.
- Determine when assessing the training program and materials:
  - The importance that the board and the senior management place on ongoing education, training and compliance
  - Employee accountability for ensuring AML/CFT compliance.
  - Comprehensiveness of training, in view of specific risks of individual business lines.
  - Participation of personnel from all applicable areas of the FI.
  - Frequency of training.
  - Coverage of FI‘s policies, procedures, processes and new rules and regulations.
  - Coverage of different forms of money laundering and terrorist financing as they relate to identifying suspicious activity.
  - Penalties for noncompliance and regulatory requirements.

4.7.6 External Auditor

External auditor shall play an essential part in reviewing the adequacy of controls by communicating their findings and recommendations to management via the annual management letter, which accompanies the audit report. External audit should focus their audit programs on risk factors and conducts intensive reviews of higher risk areas where controls may be deficient. External auditors may report incidences of suspected criminal activity uncovered during audits, to the financial sector supervisors.

CHAPTER 5: CUSTOMER DUE DILIGENCE

5.1 KNOW YOUR CUSTOMER PROGRAM

The adoption of effective Know Your Customer (KYC) program is an essential part of risk management policies. Having sufficiently verified/corrected information about customers - –Knowing Your Customer‖ (KYC) - and making use of that information underpins all AML/CFT efforts, and is the most effective defence against being used to launder the proceeds of crime.

With inadequate KYC program there may be subject to significant risks, especially legal and reputational risk. Sound KYC Policies and Procedures not only contribute to the overall safety and soundness, they also protect the integrity of its system by reducing money laundering, terrorist financing and other related offences.

5.2 KNOW YOUR CUSTOMER (KYC) PROCEDURE

Money Laundering Prevention Act, 2012 requires all reporting agencies to maintain correct and concrete information with regard to identity of its customer during the operation of their accounts. If financial institution is unable to identify the customer and verify that customer‘s identity using reliable, independent source documents, data or information, and to identify the beneficial owner, and to take reasonable measures to verify the identity of the beneficial owner and unable to obtaining information on the purpose and intended nature of the business relationship, it should not open the account, commence business relations or perform the transaction; or should terminate the business relationship; and should consider making a suspicious transactions report in relation to the customer.

5.2.1 Nature of Customer’s Business

When a business relationship is being established, the nature of the business that the customer expects to conduct with the institution should be ascertained at the outset to establish what might be expected later as normal activity. This information should be updated as appropriate, and as opportunities arise. In order to judge whether a transaction is or is not suspicious, institutions need to have a clear understanding of the business carried out by their customers.

5.2.2 Identifying Real Person

An institution must establish to its satisfaction that it is dealing with a real person (natural, corporate or legal), and must verify the identity of persons who are authorized to operate any account, or transact business for the customer. Whenever possible, the prospective customer should be interviewed personally. This will safeguard against opening of fictitious account.

5.2.3 Document is not enough

The best identification documents possible should be obtained from the prospective customer i.e. those that are the most difficult to obtain illicitly. No single piece of identification can be fully guaranteed as genuine, or as being sufficient to establish identity so verification will generally be a cumulative process. The overriding principle is that every

Branch must know who their customers are, and have the necessary documentary evidence to verify this. Collection of document is not enough for KYC, identification is very important.

5.2.4 Reliance on Third party

Third parties can be used for rely on to perform the CDD measures. The ultimate responsibility for CDD measures remains with the relying on the third party.

The criteria that should be met are as follows:

(a) HFCL relying upon a third party should immediately obtain the necessary information.

(b) It should take adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to the CDD requirements will be made available from the third party upon request without delay.

(c) It should satisfy itself that the third party is regulated, supervised or monitored for, and has measures in place for compliance with, CDD and record-keeping requirements.

5.3 COMPONENTS OF KYC PROGRAM

The KYC program should include certain key elements. Such essential elements should start from the risk management and control procedures and should include -

(1) Customer acceptance policy,

(2) Customer identification,

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

(4) Identification of suspicious transactions.

Branches should not only establish the identity of their customers, but should also monitor account activities to determine those transactions that do not conform with the normal or expected transactions for that customer or type of account. KYC should be a core feature of risk management and control procedures, and be complemented by regular compliance reviews and internal audit. The intensity of KYC programs beyond these essential elements should be tailored to the degree of risk.

5.3.1 Who is a Customer?

For the purpose of KYC Procedure a "Customer" is defined as per risk for prevention of Money Laundering and Terrorist Financing which are as follows:

- any person or institution maintaining an account of any type with a bank or financial institution or having banking related business;
- the person or institution as true beneficial owner in whose favour the account is operated;
- the trustee, intermediary or true beneficial owner of the transaction of the accounts operated by the trust and professional intermediaries (such as lawyer/law firm, chartered accountant, etc) under the existing legal infrastructure;

5.3.2 Customer Acceptance Policy

A clear customer acceptance policy and procedures should be implemented. The policy should be including laying down explicit criteria for acceptance of customers including a description of the types of customer that are likely to pose a higher than average risk. In preparing such policies, factors such as customers‘ background, country of origin, public or high profile position, linked accounts, business activities or other risk indicators should be considered.

It is important that the customer acceptance policy is not so restrictive that it results in a denial of access by the general public to financial services, especially for people who are financially or socially disadvantaged. On the other hand, quite extensive due diligence would be essential for an individual with a high net worth whose source of funds is unclear. Decisions to enter into business relationships with higher risk customers, such as public figures or politically exposed persons should be taken exclusively at senior management level.

The customer Acceptance Policy has to ensure that explicit guidelines are in place on the following aspects of customer relationship in the financial institution:

1) No account should be opened in anonymous or fictitious name.
2) Parameters of risk perception should be clearly defined in terms of the source of fund, the nature of business activity, location of customer and his clients, mode of payments, volume of turnover, service offered, social and financial status etc. to categorize customers into different risk grades.
3) Documentation requirements and other information to be collected in respect of different categories of customers depending on perceived risk.
4) Not to open an account or close an account where the financial institution is unable to apply appropriate customer due diligence measures i.e. financial institution is unable to verify the identity and/or obtain documents required as per the risk categorization due to non cooperation of the customer or non reliability of the data/information furnished to the financial institution. Decision by a financial institution to close an account should be taken at a reasonably high level after giving due notice to the customer explaining the reasons for such a decision.
5) Circumstances, in which a customer is permitted to act on behalf of another person/entity, should be clearly spelt out in conformity with the established law and practices of financial service as there could be occasions when an account is operated by a mandate holder or where an account is opened by an intermediary in fiduciary capacity.
6) Necessary checks before opening a new account to ensure that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations etc.
7) The status of a customer may change as relation with a customer progresses. The transaction pattern, volume of a customer‘s account may also change. With times an ordinary customer can turn into a risky one. To address this issue, customer acceptance policy should include measures to monitor customer‘s activities throughout the business relation

5.3.3. Customer Identification

Customer identification is an essential element of KYC standards. The customer identification process applies naturally at the outset of the relationship. To ensure that records remain up-to-date and relevant, there is a need for financial institution to undertake regular reviews of existing records. An appropriate time to do so is when a transaction of significance takes place, when customer documentation standards change substantially, or when there is a material change in the way that the account is operated. However, if a financial institution becomes aware at any time that it lacks sufficient information about an existing customer, it should take steps to ensure that all relevant information is obtained as quickly as possible.

Once verification of identity has been satisfactorily completed, no further evidence is needed to undertake subsequent transactions. However, information should be updated or reviewed as appropriate and records must be maintained as set out Chapter 6.

5.3.4 What Constitutes a Customer's Identity

Identity generally means a set of attributes which uniquely define a natural or legal person. There are two main constituents of a person's identity, remembering that a person may be any one of a range of legal persons (an individual, corporate body, partnership, etc). For the purposes of this guidance, the two elements are:

- the physical identity (e.g. Birth Certificate, TIN/VAT RegistrationPassport/National ID, Driving License etc.); and
- the activity undertaken.

Confirmation of a person's address is also useful in determining whether a customer is resident in a high-risk country. Knowledge of both residence and nationality may also be necessary, in a non money-laundering context, to avoid breaches of UN or other international sanctions to which Bangladesh is a party. Where a passport is taken as evidence, the number, date and place of issuance should be recorded.

The other main element in a person's identity is sufficient information about the nature of the business that the customer expects to undertake, and any expected or predictable, pattern of transactions. For some business these may be obvious, however, for more complex businesses this may not be the case. The extent of the description required will depend on the institution's own understanding of the applicant's business.

Once account relationship has been established, reasonable steps should be taken by the institution to ensure that descriptive information is kept up-to-date as opportunities arise. It is important to emphasize that the customer identification process does not end at the point of application. The need to confirm and update information about identity, such as changes of address, and the extent of additional KYC information to be collected over time will differ from sector to sector and between institutions within any sector. It will also depend on the nature of the product or service being offered, and whether personal contact ismaintained enabling file notes of discussion to be made or whether all contact with the customer is remote.

5.3.5 Individual Customers

Concern officer shall obtain following information while opening accounts or establishing other relationships with individual customers:

- Correct name and/or names used;
- parent's names;
- date of birth;
- current and permanent address;
- details of occupation/employment and sources of wealth or income
- Contact information, such as – mobile/telephone no.

The original, certified copy of the following Photo ID also play vital role to identify the customer:

(i) Current valid passport;

(ii) Valid driving license;

(iii) National ID Card;

(iv) Employer provided ID Card, bearing the photograph and signature of the applicant;

Identification documents which do not bear photographs or signatures, or are easy to obtain, are normally not appropriate as sole evidence of identity, e.g. birth certificate, certificate from any local

government organs, credit cards, non-Bangladeshi driving license. Any photocopies of documents showing photographs and signatures should be plainly legible. Where applicants put forward documents with which an institution is unfamiliar, either because of origin, format or language, the institution must take reasonable steps to verify that the document is indeed genuine, which may include contacting the relevant authorities or obtaining a notarized translation. Financial Institutions should also be aware of the authenticity of passports.

One or more of the following steps is recommended to verify addresses:

- provision of a recent utility bill, tax assessment or bank statement containing details of the address (to guard against forged copies it is strongly recommended that original documents are examined);
- checking the Voter lists;
- checking the telephone directory;
- visiting home/office;
- sending thanks letter.

The information obtained should demonstrate that a person of that name exists at the address given, and that the applicant is that person.

5.3.5.1 No face-to-face contact: Where there is no face-to-face contact, photographicidentification would clearly be inappropriate procedures to identify and authenticate the customer. Branch should ensure that there is sufficient evidence, either documentary or electronic, to confirm address and personal identity. At least one additional check should beundertaken to guard against impersonation. In the event that internal procedures require sight of a current passport or ID card where there is no face-to-face contact, then a certified true copy should be obtained. Branch should not allow non face to face contact to a resident in establishing relationship.

5.3.5.2 Appropriateness of documents: There is obviously a wide range of documentswhich might be provided as evidence of identity. It is for each institution to decide the appropriateness of any document in the light of other procedures adopted. However, particular care should be taken in accepting documents which are easily forged or which can be easily obtained using false identities.

5.3.5.3 Joint Accounts: In respect of joint accounts where the surname and/or address ofthe account holders differ, the name and address of all account holders, not only the first named, should normally be verified in accordance with the procedures set out above.

5.3.5.4 Change in address or other details: Any subsequent change to the customer‘sname, address, or employment details of which the financial institution becomes aware should be recorded as part of the Know Your Customer process. Generally this would be undertaken as part of good business practice and due diligence but also serves for money laundering prevention.

5.3.5.5 Record keeping: All documents collected or gathered for establishing relationshipmust be filed in with supporting evidence. Where this is not possible, the relevant details should be recorded on the applicant's file. Institutions which regularly conduct one-off transactions, should record the details in a manner which allows cross reference to transaction records.

5.3.5.6 Introducer: To identify the customer and to verify his/her identity, an introducer may play important role. An introduction from a respected customer, personally known to the management, or from a trusted member of staff, may assist the verification procedure but does not replace the need for verification of address as set out above. Details of the introduction should be recorded on the customer's file. However, personal introductions without full verification should not become the norm, and directors/senior managers must not require or request staff to breach account opening procedures as a favor to an applicant.

5.3.5.7 Persons without Standard Identification Documentation

It is generally believed that financial inclusion is helpful in preventing money laundering and terrorist financing. Most people need to make use of the financial system at some point in their lives. It is important, therefore, that the socially or financially disadvantaged such as the elderly, the disabled, students and minors should not be precluded from obtaining financial services just because they do not possess evidence of identity or address where they cannot reasonably be expected to do so. In these circumstances, a common sense approach and some flexibility without compromising sufficiently rigorous AML procedures is recommended. Internal procedures must allow for this, and must provide appropriate advice to staff on how identity can be confirmed in these exceptional circumstances. The important point is that a person's identity can be verified from an original or certified copy of another document, preferably one with a photograph. FIs shall not allow ‗high value' transactions to this kind of customers.

A certifier must be a suitable person, such as for instance a lawyer, accountant, director or manager of a regulated institution, a notary public, a member of the judiciary or a seniorcivil servant. The certifier should sign the copy document (printing his name clearly underneath) and clearly indicate his position or capacity on it together with a contact address and phone number.

In these cases it may be possible for the institution to accept confirmation from a professional (e.g. doctor, lawyer, directors or managers of a regulated institution, etc) who knows the person. Where the individual lives in accommodation for which he or she is not financially responsible, or for which there would not be documentary evidence of his/her address, it may be acceptable to accept a letter from the guardian or a similar professional as confirmation of a person's address. A manager may authorize the opening of a business relationship if s/he is satisfied with confirmation of identity circumstances but must record his/her authorization on the customer's file, and must also retain this information in the same manner and for the same period of time as other identification records.

5.3.5.8 Minor

For minor, the normal identification procedures set out above should be followed as far as possible. Where such procedures would not be relevant, or do not provide satisfactory evidence of identity, verification might be obtained in the form of the home address of parent(s). Under normal circumstances, a family member or guardian who has an existing relationship with the institution concerned would introduce a minor. In cases where the person opening the account is not already known, the identity of that person, and any other person who will have control of the account, should be verified.

5.3.6 Corporate Bodies and Other Entities

Because of the difficulties of identifying beneficial ownership, and the possible complexity of organization and structures, corporate entities and trusts are the most likely vehicles to be used for money laundering, particularly when a legitimate trading company is involved. Particular care should be taken to verify the legal existence of the applicant and to ensure that any person purporting to act on behalf of the applicant is authorized to do so. The principal requirement is to look behind a corporate entity to identify those who have ultimate control over the business and the company's assets, with particular attention being paid to any shareholders or others who exercise a significant influence over the affairs of the company. Enquiries should be made to confirm that the company exists for a legitimate trading or economic purpose, and that it is not merely a ―brass plate company‖ where the controlling principals cannot be identified.

Before a business relationship is established, measures should be taken by way of company search and/or other commercial enquiries to ensure that the applicant company has not been, or is not in the process of being, dissolved, and struck off, wound-up or terminated. In addition, if the institution

becomes aware of changes in the company structure or ownership, or suspicions are aroused by a change in the nature of business transacted, further checks should be made.

No further steps to verify identity over and above usual commercial practice will normally be required where the applicant for business is known to be a company, or a subsidiary of a company, quoted on a recognized stock exchange.

The following documents should normally be obtained from companies:

- Certified copy of Certificate of Incorporation or equivalent, details of the registered office, and place of business;
- Certified copy of the Memorandum and Articles of Association, or by-laws of the client.
- Copy of the board resolution to open the account relationship and the empowering authority for those who will operate any accounts;
- Explanation of the nature of the applicant's business, the reason for the relationship being established, an indication of the expected turnover, the source of funds, and a copy of the last available financial statements where appropriate;
- Satisfactory evidence of the identity of each of the principal beneficial owners being any person holding 10% interest or more or with principal control over the company‘s assets and any person (or persons) on whose instructions the signatories on the account are to act or may act where such persons are not full time employees, officers or directors of the company;
- Satisfactory evidence of the identity of the account signatories, details of their relationship with the company and if they are not employees an explanation of the relationship. Subsequent changes to signatories must be verified;
- Copies of the list/register of directors.

Where the business relationship is being opened in a different name from that of the applicant, the institution should also satisfy itself that the reason for using the second name makes sense.

The following persons (i.e. individuals or legal entities) must also be identified in line with this part of the notes:

- All of the directors who will be responsible for the operation of the account / transaction.
- All the authorized signatories for the account/transaction.
- All holders of powers of attorney to operate the account/transaction.
- The beneficial owner(s) of the company
- The majority shareholders of a private limited company.

A letter issued by a corporate customer is acceptable in lieu of passport or other photo identification documents of their shareholders, directors and authorized signatories. Where the institution already knows their identities and identification records already accord with the requirements of these notes, there is no need to verify identity again.

When authorized signatories change, care should be taken to ensure that the identities of all current signatories have been verified. In addition, it may be appropriate to make periodic enquiries to establish whether there have been any changes in directors/shareholders, or the nature of the business/activity being undertaken. Such changes could be significant in relation to potential money laundering activity, even though authorized signatories have not changed.

5.3.6.1 Companies Registered Abroad

Particular care should be exercised when establishing business relationships with companies incorporated or registered abroad, or companies with no direct business link to Bangladesh. Such

companies may be attempting to use geographic or legal complication to interpose a layer of opacity between the source of funds and their final destination. In such circumstances, institutions should carry out effective checks on the source of funds and the nature of the activity to be undertaken during the proposed business relationship. This isparticularly important if the corporate body is registered or has known links to countries without anti-money laundering legislation and procedures equivalent to Bangladesh. In the case of a trading company, a visit to the place of business may also be made to confirm the true nature of the business.

5.3.7 Partnerships and Unincorporated Businesses

In the case of partnerships and other unincorporated businesses whose partners/directors are not known to the institution, the identity of all the partners or equivalent should be verified in line with the requirements for personal customers. Where a formal partnership agreement exists, a mandate from the partnership authorizing the opening of an account and conferring authority on those who will operate it should be obtained.

Evidence of the trading address of the business or partnership should be obtained and a copy of the latest report and accounts (audited where applicable).

An explanation of the nature of the business or partnership should be ascertained (but not necessarily verified from a partnership deed) to ensure that it has a legitimate purpose.

5.3.8 Powers of Attorney/ Mandates to Operate Accounts

The authority to deal with assets under a power of attorney constitutes a business relationship and therefore, where appropriate, it may be advisable to establish the identities of holders of powers of attorney, the grantor of the power of attorney and third party mandates. Records of all transactions undertaken in accordance with a power of attorney should be kept.

5.3.9 KYC for Internet or Online Based Customer

Banking and investment business through the Internet add a new dimension to Financial Institutions' activities. The unregulated nature of the Internet is attractive to criminals, opening up alternative possibilities for money laundering and fraud.

It is recognized that on-line account opening services are convenient. However, it is not appropriate that Financial Institutions should offer on-line live account opening allowing full immediate operation of the account in a way which would dispense with or bypass normal identification procedures.

However, initial application forms could be completed on-line and then followed up with appropriate identification checks. The account, in common with accounts opened through more traditional methods, should not be put into full operation until the standardized account opening provisions have been satisfied in accordance with these Guidance Notes.

The development of technologies such as encryption, digital signatures, etc., and the development of new financial services and products, makes the Internet a dynamic environment offering significant business opportunities. The fast pace of technological and product development has significant regulatory and legal implications, and Bangladesh Bank is committed to keeping up-to-date with any developments on these issues through future revisions to its Guidance Notes.

5.3.10 Timing and Duration of Verification

The best time to undertake verification is prior to entry into the account relationship. Verification of identity should, as soon as is reasonably practicable, be completed before any transaction is completed.

However, if it is necessary for sound business reasons to open an account or carry out a significant one-off transaction before verification can be completed, this should be subject to stringent controls which should ensure that any funds received are not passed to third parties. Alternatively, a senior member of staff may give appropriate authority.

This authority should not be delegated, and should only be done in exceptional circumstances. Any such decision should be recorded in writing.

Verification, once begun, should normally be pursued either to a satisfactory conclusion or to the point of refusal. If a prospective customer does not pursue an application, staff may (or may not) consider that this is itself suspicious.

5.4 KNOW YOUR EMPLOYEE (KYE)

A Know Your Employee (KYE) program in place that allows it to understand an employee‘s background, conflicts of interest and susceptibility to money laundering complicity. Policies, procedures, internal controls, job description, code of conduct/ethics, levels of authority, compliance with personnel laws and regulations, accountability, dual control, and other deterrents should be firmly in place.

Background screening of prospective and current employees, especially for criminal history, is essential to keep out unwanted employees and identifying those to be removed. It can be an effective risk management tool, providing management with some assurance that the information provided by the applicant is true and that the potential employee has no criminal record. Used effectively, the pre-employment background checks may reduce turnover by verifying that the potential employee has the requisite skills, certification, license or degree for the position; deter theft and embezzlement; and prevent litigation over hiring practices. An institution should verify that contractors are subject to screening procedures similar to its own.

The sensitivity of the position or the access level of an individual employee may warrant additional background screening, which should include verification of references, experience, education and professional qualifications. The extent of the screening depends on the circumstances, with reasonableness the standard

.

CHAPTER 6: RECORD KEEPING

6.1 STATUTORY REQUIREMENT

The requirement contained in Section 25 (1) of Money Laundering Prevention Act, 2012, to retain correct and full records of customers' identification and transactions while operating an account of a customer, and to retain the records of customers' identification and transactions at least for five years after closing of relationships with the customers are essential constituents of the audit trail that the law seeks to establish.

As per MLPA 2012 HFCL will maintain, for at least five years, all necessary records on transactions, both domestic and international, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved, if any) so as to provide, if necessary, evidence for prosecution of criminal activity.

The records prepared and maintained by any Branches on its customer relationship and transactions should be such that:

- requirements of legislation and Bangladesh Bank directives are fully met;
- competent third parties will be able to assess the institution's observance of money laundering policies and procedures;
- any transactions effected via the institution can be reconstructed;
- any customer can be properly identified and located;
- all suspicious reports received internally and those made to Bangladesh Bank can be identified; and
- the institution can satisfy within a reasonable time any enquiries or court orders from the appropriate authorities as to disclosure of information.

Records relating to verification of identity will generally comprise:

- a description of the nature of all the evidence received relating to the identity of the verification subject;
- the evidence itself or a copy of it or, if that is not readily available, information reasonably sufficient to obtain such a copy.

Records relating to transactions will generally comprise:

- details of personal identity, including the names and addresses, etc. pertaining to:
  (1) the customer;
  (2) the beneficial owner of the account or product;
  (3) the non-account holder conducting any significant one-off transaction;
  (4) any counter-party;
- details of transaction including:
  1) nature of such transactions;
  2) volume of transactions customer's instruction(s) and authority(ies);
  3) source(s) of funds;
  4) destination(s) of funds;
  5) book entries;
  6) custody of documentation;

7) date of the transaction;
8) form in which funds are offered and paid out.
9) parties to the transaction
10) identity of the person who conducted the transaction on behalf of the customer

These records of identity must be kept for at least five years from the date when the relationship with the customer has ended. This is the date of:

i. closing of an account

ii. providing of any financial services

iii. carrying out of the one-off transaction, or the last in a series of linked one-off transactions; or

iv. ending of the business relationship; or

v. commencement of proceedings to recover debts payable on insolvency.

Branches should ensure that records pertaining to the identification of the customer, his/her address (e.g. copies of documents like passport, national ID card, driving licence, trade licence, utility bills etc.) obtained while opening the account and during the course of business relationship, are properly preserved for at least five years after the business relationship is ended and should be made available to the competent authorities upon request without delay.

6.2 RETRIEVAL OF RECORDS

To satisfy the requirements of the law and to meet the purpose of record keeping, it is important that records are capable of retrieval without undue delay. It is not necessary to retain all the documents relating to customer identity and transaction physically at the premises of the branch of a financial institution, provided that they have reliable procedures for keeping the hard copy at a central archive, holding records in electronic form, and that can be reproduced and recollected without undue delay.

It is not always necessary to retain documents in their original hard copy form, provided that the firm has reliable procedures for holding records in microchips or electronic form, as appropriate, and that these can be reproduced without undue delay. In addition, an institution may rely on the records of a third party, such as a bank or clearing house in respect of details of payments made by customers. However, the primary requirement is on the institution itself and the onus is thus on the business to ensure that the third party is willing and able to retain and, if asked to, produce copies of the records required.

However, the record requirements are the same regardless of the format in which they are kept or whether the transaction was undertaken by paper or electronic means. Documents held centrally must be capable of distinguishing between the transactions relating to different customers and of identifying where the transaction took place and in what form.

6.3 STR RELATED INSPECTION AND INVESTIGATION

Where a report submitted as suspicious transaction to BFIU or where it is known that a customer or any transaction is under investigation, it should not destroy any records related to the customer or transaction without the consent of the BFIU or conclusion of the case even though the five-year limit may have been elapsed. To ensure the preservation of such records the financial institutions should maintain a register or tabular records of all investigations and inspection made by the investigating authority or Bangladesh Bank and all disclosures to the BFIU. The register should be kept separate from other records and contain as a minimum the following details:

i. the date of submission and reference of the STR/SAR;

ii. the date and nature of the enquiry;

iii. the authority who made the enquiry, investigation and reference; and

iv. details of the account(s) involved.

6.4 TRAINING RECORDS

HFCL will comply with the regulations concerning staff training, they shall maintain training records which include:-

(i) details of the content of the training programs provided;

(ii) the names of staff who have received the training;

(iii) the date/duration of training;

(iv) the results of any testing carried out to measure staffs understanding of the requirements; and

(v) an on-going training plan.

6.5 BRANCH LEVEL RECORD KEEPING

To ensure the effective monitoring and demonstrate their compliance with the concerned regulations, Branch have to ensure the keeping or availability of the following records at the branch level either in hard form or electronic form:

1) Information regarding Identification of the customer,
2) KYC information of a customer,
3) Transaction report,
4) Suspicious Transaction/Activity Report generated from the branch,
5) Exception report,
6) Training record,
7) Return submitted or information provided to the Head Office or competent authority.

6.6 SHARING OF RECORD/INFORMATION OF/TO A CUSTOMER

Under MLPA 2012, and ATA, 2009 (as amended in 2012), Any Officer/Executive shall not share account related information to investigating authority i.e., ACC or person authorized by ACC to investigate the said cases without having court order or prior approval from Bangladesh Bank.

CHAPTER 7: SUSPICIOUS TRANSACTION REPORT/SUSPICIOUS ACTIVITY REPORT

The final output of all compliance programs is reporting of suspicious transaction or reporting of suspicious activity. Suspicious Transaction Report (STR) or Suspicious Activity Report (SAR) is an excellent tool for mitigating or minimizing the risk. So it is necessary for the safety and soundness of our organization.

7.1 DEFINITION OF STR/SAR

Generally STR/SAR means a formatted report of suspicious transactions/activities where there are reasonable grounds to suspect that funds are the proceeds of predicate offence or may be linked to terrorist activity or the transactions do not seem to be usual manner. Such report is to be submitted by financial institutions to the competent authorities.

In the section (2)(z) of MLPA, 2012 ―suspicious transaction‖ means such transactions which deviates from usual transactions; of which there is ground to suspect that,

(1) the property is the proceeds of an offence,

(2) it is financing to any terrorist activity, a terrorist group or an individual terrorist;

(3) which is, for the purposes of this Act, any other transaction or attempt of transaction delineated in the instructions issued by Bangladesh Bank from time to time.

In Anti Terrorism Act, 2009 (as amended in 2012), STR/SAR refers to the transaction that relates to financing for terrorism or terrorist individual or entities. One important thing is that financial institutions (hereafter branches of HFCL) need not to establish any proof of occurrence of a predicate offence; it is a must to submit STR/SAR only on the basis of suspicion.

7.2 OBLIGATIONS OF SUCH REPORT

As per the Money Laundering Prevention Act, 2012, Branches are obligated to submit STR/SAR to Bangladesh Bank. Such obligation also prevails for the HFCL in the Anti Terrorism Act, 2009 (as amended in 2012). Other than the legislation, Bangladesh Bank has also instructed to submit STR/SAR through AML Circulars issued by Bangladesh Bank time to time.

7.3 REASONS FOR REPORTING OF STR/SAR

As discussed above, STR/SAR is very crucial for the safety and soundness of the financial institutions. The Branches should submit STR/SAR considering the followings:

- It is a legal requirement in Bangladesh;
- It helps protect the reputation of HFCL ;
- It helps to protect HFCL from unfounded allegations of assisting criminals, including terrorists;
- It helps the authorities to investigate money laundering, terrorist financing, and other financial crimes.

7.4 IDENTIFICATION AND EVALUATION STR/SAR

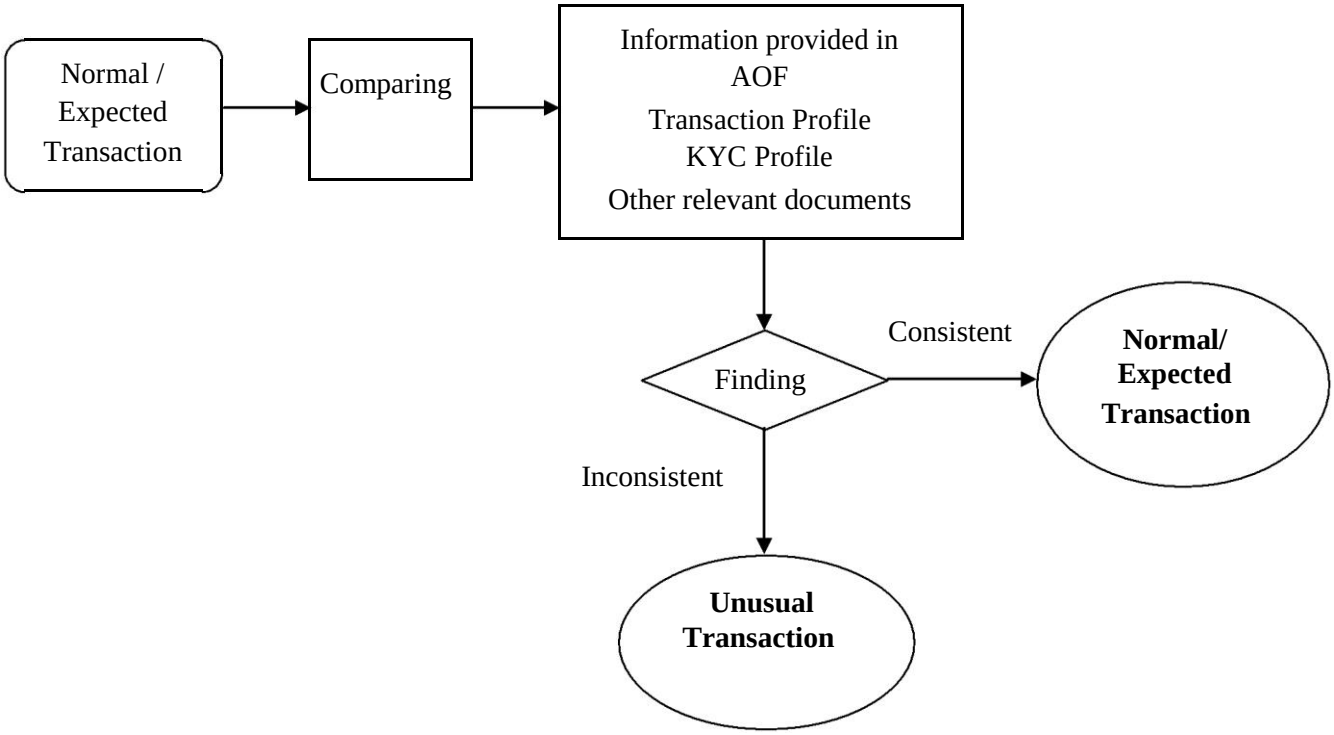
Identification of STR/SAR is very crucial for mitigate the risk. Identification of STR/SAR depends upon the detection mechanism in place by the Branches. Such suspicion may not only at the time of transaction but also at the time of doing KYC and attempt to transaction.

7.4.1 Identification of STR/SAR:

Identification of STR/SAR may be started identifying unusual transaction and activity. Such unusual transaction may be unusual in terms of complexity of transaction, nature of transaction, volume of transaction, time of transaction etc. Generally the detection of unusual transactions/activities may something be sourced as follows:

- Comparing the KYC profile, if any inconsistency is found and there is no valid reasonable explanation.
- By monitoring customer transactions.
- By using red flag indicator.

Simply, if any transaction/activity is consistent with the provided information by the customer can be treated as normal and expected. When such transaction/activity is not normal and expected, it may treat as unusual transaction/activity.



As discussed above, the identification of STR/SAR may be sourced from unusual transaction or activity. In case of reporting of STR/SAR, FIs should conduct the following 3 stages:

a) Identification:

This stage is very vital for STR/SAR reporting. Depending on size, need and complexity of financial institutions monitoring of unusual transactions may be automated, manually or both. Some financial institutions use specialized software to detect unusual transactions or activities, however, the use of such software can only be complemented managerial oversight and not be replaced the need for constant monitoring of activity of the accounts of customers. Monitoring mechanisms should be more rigorous in high-risk areas of an institution and supported by adequate information systems to alert management and other appropriate staff (e.g., the compliance officer) of unusual /suspicious activity. Training of staff in the identification of unusual /suspicious activity should always be an ongoing activity. Considering the nature of business FIs must be vigilant in KYC and sources of funds of the customer to identify STR/SAR.

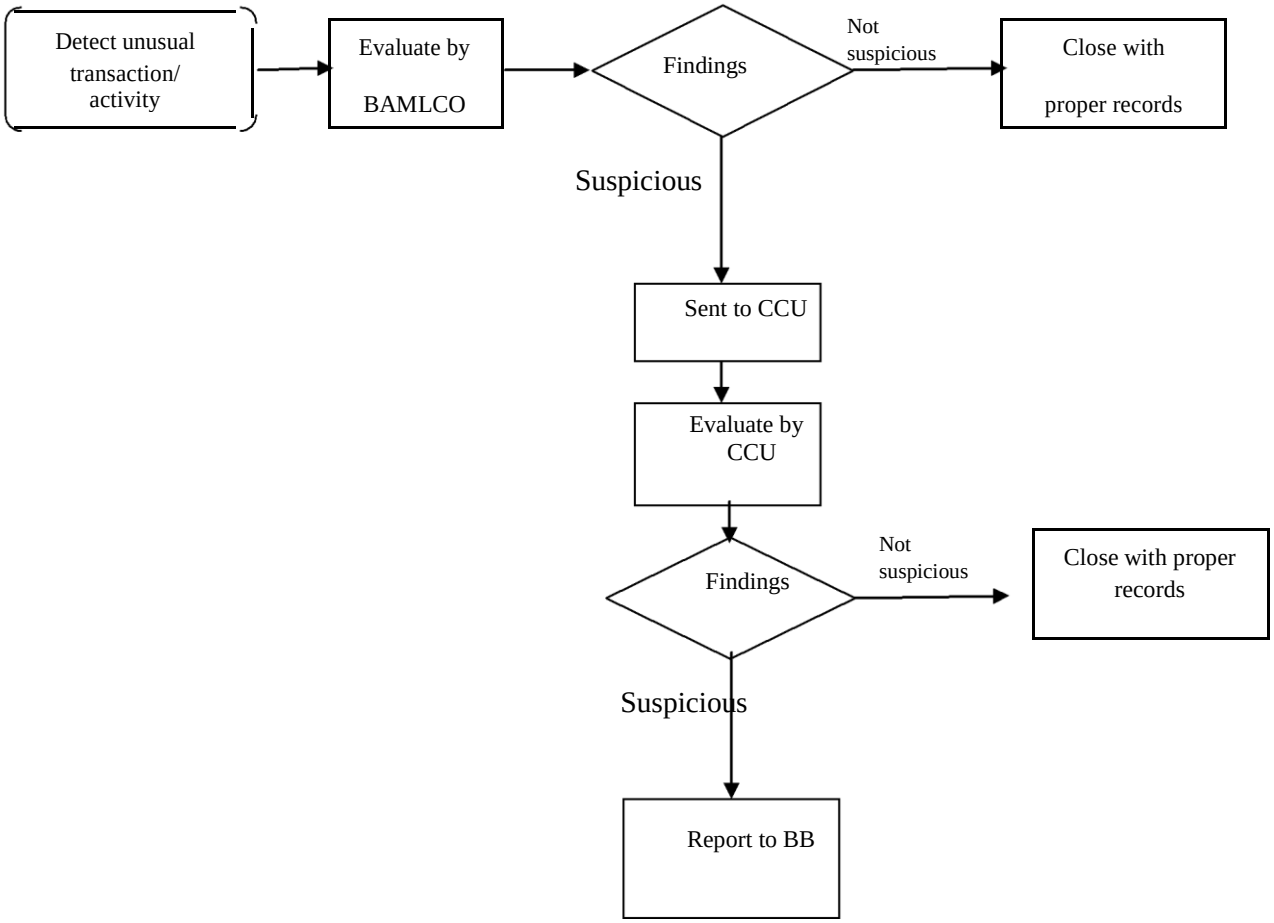
b) Evaluation:

These problems will be in place at branch level and Central Compliance Unit (CCU). After identification of STR/SAR by any branch officers he/she will inform BAMLCO in written, BAMLCO will evaluate the transaction/activity to identify suspicion by interviewing the customer or through any other means. In evaluation stage concerned BAMLCO must be tactful considering the tipping off provision of the acts. If BAMLCO is not satisfied, he should forward the report to CCU. After receiving report from branch CCU should also evaluate the report whether the STR/SAR report should be sent to BFIU or not. At every stages of evaluation (whether reported to Bangladesh Bank or not) financial institutions should keep records with proper manner.

c) Disclosure:

This is the final stage and branch officers should submit STR/SAR to CCU if it is still suspicious.

For simplification the flow chart given below shows STR/SAR identification and reporting procedures:



7.5 RISK-BASED APPROACH

An integrated risk-based system depends mainly on a proper assessment of the relevant risk sectors, products, services, and clients and on the implementation of appropriate risk-focused due diligence and record-keeping. These in turn become the foundation for monitoring and compliance mechanisms that allow rigorous screening of high-risk areas and accounts. Without sufficient due diligence and risk profiling of a customer, adequate monitoring for suspicious activity would be impossible. According to the Wolfsberg Group guidelines, a risk-based monitoring system for financial institutions clients should:

- compare the clients account/transaction history to the clients specific profile information and a relevant peer group, and/or examine the clients account/transaction history against established money-laundering criteria/scenarios, in order to identify patterns of suspicious activity or anomalies;
- establish a process to compare customer or transaction-specific data against risk-scoring models;
- be capable of recognizing patterns and of –learning‖ which transactions are normal for a client, rather than designating certain transactions as unusual (for example, not all large transaction are unusual and may easily be explained);
- issue alerts if unusual transactions are identified;
- track alerts in order to ensure they are appropriately managed within the institution and that suspicious activity is reported to the authorities as required; and
- maintain an audit trail for inspection by the institution's audit function and by financial institutions supervisors.

7.6 REPORTING OF STR/SAR

HFCL enlisted as per MLPA, 2012 and ATA, 2009 (as amended in 2012) are obligated to submit STR/SAR to Bangladesh Bank. Such report must come to the Bangladesh Bank from CCU of the respective institutions by using specified format/instruction given by the Bangladesh Bank.

7.7 TIPPING OFF

Section 6 of MLPA 2012 and FATF Recommendation 21 prohibits financial institution, their directors, officers and employees from disclosing the fact that an STR or related information is being reported to BFIU. A risk exists that customers could be unintentionally tipped off when the branch is seeking to perform its CDD obligation in those circumstances. The customer‘s awareness of a possible STR or investigation could compromise future effort to investigate the suspected money laundering or terrorist financing operation.

7.7.1 Penalties of Tipping Off

Under section 6 of MLPA, 2012, if any person, institution or agent empowered under this Act divulges any information collected, received, retrieved or known by the person, institution or agent during the course of employment or appointment, or after the expiry of any contract of service or appointment for any purpose other than the purposes of this Act shall be punished with imprisonment for a term not exceeding 2 (two) years or a fine not exceeding taka 50 (fifty) thousand or with both.

7.8 “SAFE HARBOR” PROVISIONS FOR REPORTING

Safe harbor laws encourage financial institutions to report all suspicious transactions by protecting institutions and employees from criminal and civil liability when reporting suspicious transactions in good faith to competent authorities. In section (28) of MLPA, 2012 provides the safe harbor for reporting.

7.9 RED FLAGS OR INDICATORS OF STR

7.9.1 Moving Customers: A customers who moves every month, particularly if there isnothing in that person‘s information suggesting that frequent changes in residence is normal, could be suspicious.

7.9.2 **Out of market windfalls**: If you think a customer who just appeared at yourbranch/offices sounds too good to be true, you might be right. Pay attention to one whose address is far from your office, especially if there is no special reason why you were given the business. Aren‘t there bank/FI closer to home that could provide the service? If the customer is a business, the distance to its operations may be an attempt to prevent you from verifying there is no business after all. Don‘t be bullied by your sales personnel who follow the ―no question asked‖ philosophy of taking in new business.

7.9.3 Suspicious Customer Behavior:

- Customer has an unusual or excessively nervous demeanor.
- Customer discusses your record-keeping or reporting duties with the apparent intention of avoiding them.
- Customer threatens an employee in an effort to discourage required record-keeping or reporting.
- Customer is reluctant to proceed with a transaction after being told it must be recorded.
- Customer appears to have a hidden agenda or behaves abnormally, such as turning down the chance to obtain a higher profit rate on a large account balance.
- Customer who is a public official opens account in the name of a family member who begins making large deposits not consistent with the known source of legitimate family income.
- Customer who is a student uncharacteristically transacts large sums of money.
- Agent, attorney or financial advisor acts for another person without proper documentation such as a power of attorney.

7.10.1 Suspicious Customer Identification Circumstances:

- Customer furnishes unusual or suspicious identification documents and is unwilling to provide personal data.
- Customer is unwilling to provide personal background information when opening an account.
- Customer‘s permanent address is outside the HFCL‘s service area.
- Customer asks many questions about how the financial institution disseminates information about the identification of a customer.
- A business customer is reluctant to reveal details about the business activities or to provide financial statements or documents about a related business entity.

7.10.2 Suspicious Cash Transactions:

- Customer opens several accounts in or more names, then makes several cash deposits under the reporting threshold.
- Customer conducts large cash transactions at different branches on the same day, or orchestrates persons to do so in his/her behalf.
- Corporate account has deposits and withdrawals primarily in cash than cheques.

7.10.3 Suspicious Non-Cash Deposits:

- Customer deposits large numbers of consecutively numbered money orders or round figure amounts.
- Customer deposits cheques and/or money orders that are not consistent with the intent of the account or nature of business.

- Funds out of the accounts are not consistent with normal business or personal items of the account holder
- Funds deposited are moved quickly out of the account via payment methods inconsistent with the established purpose of the account.

7.10.4 Suspicious Activity in Credit Transactions:

- A customer‘s financial statement makes representations that do not conform to accounting principles.
- Customer suddenly pays off a large problem loan with no plausible explanation of source of funds.
- Customer purchases certificates of deposit and uses them as collateral for a loan.

7.10.5 Suspicious Commercial Account Activity:

- Business customer presents financial statements noticeably different from those of similar businesses.
- Large business presents financial statements that are not prepared by an accountant.

7.10.6 Suspicious Employee Activity:

- Employee exaggerates the credentials, background or financial ability and resources of a customer in written reports the FI requires.
- Employee frequently is involved in unresolved exceptions or recurring exceptions on exception reports.
- Employee lives a lavish lifestyle that could not be supported by his/her salary.
- Employee frequently overrides internal controls or established approval authority or circumvents policy.

7.10.7 Suspicious Activity in an FI Setting:

- Request of early encashment.
- A DPS (or whatever) calling for the periodic payments in large amounts.
- Lack of concern for significant tax or other penalties assessed when cancelling a deposit.

CHAPTER 8: CASH TRANSACTION REPORT (CTR)

Branch will analysis its daily transaction monthly, if any client transact any amount in one day in one or multiple transaction deposit or withdrawn (including one line fund transfer) equivalent to or more than Tk. 10,00,000/- (Ten Lac), branch will submit the Cash Transaction Report (CTR) to Central Compliance Unit for onward submission to BFIU. Cash transaction means any cash transaction in HFCL Bank Account by way of deposit or withdraws by HFCL's client or third party.

The CTR will be submitted to CCU in each month within 15th of the following month. CCU will upload the report through web to goAML.

Any cash transaction will not be considered as Suspicious Transaction. But Central Compliance Unit can identify any transaction as STR by analyzing the transaction mode and if they find fit then the transaction may be submitted to BFIU as Suspicious Transaction. The CAMLCO will issue a certificate if no STR is found in any monthly transaction analysis and this certificate will be submitted to BFIU via GOAML.

If any month there is no reportable CTR of STR, then a certificate "No Reportable Cash Transaction is found this month" will be submitted goAML via Message Board.

Each branch will preserve the Monthly Cash Transaction Report.

Cash transaction report will be preserved for next 5(five) years after submission of the report.

List of Abbreviations

AML/CFT	Anti-Money Laundering/Combating the Financing of Terrorism
AMLD	Anti-Money Laundering Department
APG	Asia Pacific Group on Money Laundering
ATA	Anti Terrorism Act
BAMLCO	Branch Anti-Money Laundering Compliance Officer
BB	Bangladesh Bank
BDT	Bangladesh Taka
BFIU	Bangladesh Financial Intelligence Unit
CAMLCO	Chief Anti-Money Laundering Compliance Officer
CCU	Central Compliance Unit
CDD	Customer Due Diligence
CTC	Counter Terrorism Committee
CTR	Cash Transaction Report
FATF	Financial Actions Task Force
FI	Financial Institution
FIU	Financial Intelligence Unit
FSRB	FATF Style Regional Body
GPML	Global program against Money Laundering
ICRG	International Cooperation and Review Group
IOSCO	International Organization of Securities Commissions
KYC	Know Your Customer
ML	Money Laundering
MLPA	Money Laundering Prevention Act
NCC	National Coordination Committee on
NCCT	Non-cooperating Countries and Territories
OECD	Organization for Economic Co-operation and Development
PEP	Politically Exposed Persons
SAR	Suspicious Activity Report
STR	Suspicious Transaction Report
TF	Terrorist Financing
TP	Transaction Profile
UN	United Nations
UNODC	UN Office of Drugs and Crime
UNSCR	United Nations Security Council Resolution