MERIDIAN FINANCE & INVESTMENT LIMITED

GUIDELINES ON PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING

Version – 2.0

MARCH, 2017

DOCUMENT AUTHORISATION

Document Title	Guidelines On Prevention Of Money Laundering And Terrorist Financing
Policy Reference	
Version	2.0
Date	March, 2017
Owner	Central Compliance Unit

POLICY DEVELOPMENT HISTORY

Author	Irteza Ahmed Khan, Deputy Managing Director & CAMLCO
Policy Approved By	
Board of Directors in its 15th Meeting held on March 13, 2017	

PREFACE

Money Laundering is a serious threat to financial system of all countries and it leads to destruction of the country's financial market, payment mechanism, and infrastructure and endanger the country's sovereignty as a whole. Nowadays Money Laundering and Terrorist financing has emerged as the alarming financial crime in the global economy. To combat with these, Government of Bangladesh has enacted the "Money Laundering Prevention Act 2012 *(as amended in 2015)*" and "*Anti-Terrorism Act 2009 (as amended in 2012)".* Besides, Bangladesh Bank vides DFIM circular #7 dated 4 October, 2012 has declared 'Money laundering and Terrorist Financing Risk' as one of the core risks of the financial institutions. In this regard, Bangladesh Financial Intelligence Unit (BFIU) has also issued 'Guidance Note on prevention of money laundering and terrorist financing'. In this context, Meridian Finance & Investment Limited (referred as "MFIL") prepares its own policy named hereafter "Guidelines on Prevention of Money Laundering and Terrorist Financing".

Good compliance is generally best facilitated by a willing adoption the regime of best practice; MFIL, as a whole, would aim at this while implementing this policy.

To ensure compliance with these enactments, MFIL established a Central Compliance Unit (CCU) (Sec: 3.1) under the leadership of CAMLCO who is not lower than the third rank in seniority in organizational hierarchy. Besides, MFIL has designated one high level officer as Deputy Chief Anti-Money Laundering Compliance Officer (Deputy CAMLCO) in the CCU and Branch Anti-Money Laundering Compliance Officer (BAMLCO) in the branch level. The CAMLCO is the Head of CCU and has vast working experience which is more than required.

Compliance requirements of the above enactments which MFIL or its employees should always bear in mind are as follows:

1. Report to BFIU proactively and immediately, facts on suspicious, unusual or doubtful transactions (STR/SAR) likely to be related to money laundering. [Ref:25(1)(d) of MLPA 2012]
2. Maintain confidentiality while sharing customer's account related information. [Ref: MLPA 2012 and ATA 2009 (as amended in 2012)]
3. Not to disclose the fact that an STR or related information is being reported to BFIU. [Ref: Sec 6 of MLPA 2012 and FATF Recommendation #21]
4. Not to open or maintain numbered or anonymous account
5. Know your employee (KYE) and Know your customer(KYC)
6. Exercising enhanced due diligence (annexure: 3) while opening accounts of PEPs.[ML circular # 14 dated 25 September2007]
7. Customer Due Diligence (Chapter 5) should be exercised in the case of customer identification, acceptance, monitoring and reporting of suspicious transactions.
8. Self-assessment of the effectiveness of the ML / TF program should be carried on half yearly by the ML Compliance Officers and the results of the same to be communicated to the Head of CCU. [ML circular #15]
9. Both the ICC division and external auditors of the company have apply independent testing procedure to check the adequacy of ML controls/policies. [ML circular #15]

10. Maintain, for at least five years, all necessary records on transactions, to comply with information requests from the competent authorities [U/s 25(1) of MLPA 2012]. However as per MFIL's Document Retention Policy the same to be maintained for at least fifteen years.

The rest of the chapters have been developed in line with the compliance requirements of the above enactments as well as continuing business needs. Every employee of MFIL has a duty to understand and comply with this policy and hence a declaration to that effect has to be obtained by the HR from every employee.

Table of Contents

Chapter One: Introduction

Money Laundering is being employed by launderers worldwide to conceal the proceeds earned from criminal activities. It happens in almost every country in the world, and a single scheme typically involves transferring money through several countries in order to obscure its origins. And the rise of global financial markets makes money laundering easier than ever, making it possible to anonymously deposit "dirty" money in one country and then have it transferred to any other country for use.

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. To address these emerging challenges, the global community has taken various initiatives against ML/TF. In accordance with international initiatives, Bangladesh has also acted on many fronts.

1.1 Defining Money Laundering

Money laundering can be defined in a number of ways. Most countries subscribe to the definition adopted by the United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988) (Vienna Convention)1 and the United Nations Convention Against Transnational Organized Crime (2000) (Palermo Convention):

- The conversion or transfer of property, knowing that such property is derived from any [drug trafficking] offense or offenses or from an act of participation in such offense or offenses, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an offense or offenses to evade the legal consequences of his actions;

- The concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property, knowing that such property is derived from an offense or offenses or from an act of participation in such an offense or offenses, and;

- The acquisition, possession or use of property, knowing at the time of receipt that such property was derived from an offense or offenses or from an act of participation in such offense or offenses

The Financial Action Task Force (FATF), which is recognized as the international standard setter for anti-money laundering (ML) efforts, defines the term ―money laundering succinctly as ―the processing of criminal proceeds to disguise their illegal origin in order to ―legitimize the ill-gotten gains of crime.

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

1.2 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 Purpose of Money Laundering:

The purpose of money laundering is to break the connection between the money and the crime that generated the money. In other words, money laundering disguises or conceals the illicit origin of money generated by criminal activities.

Criminals engage in money laundering for three main reasons:

i. Money is required to organize and run criminal activity for financial gain. Because it covers operating expenses, replenishes inventories, purchases the services of corrupt officials to escape detection and supplements finance for new crimes. It also pays the criminals for an expensive lifestyle. To spend money in these ways, criminals must make the money they derived illegally appear legitimate.

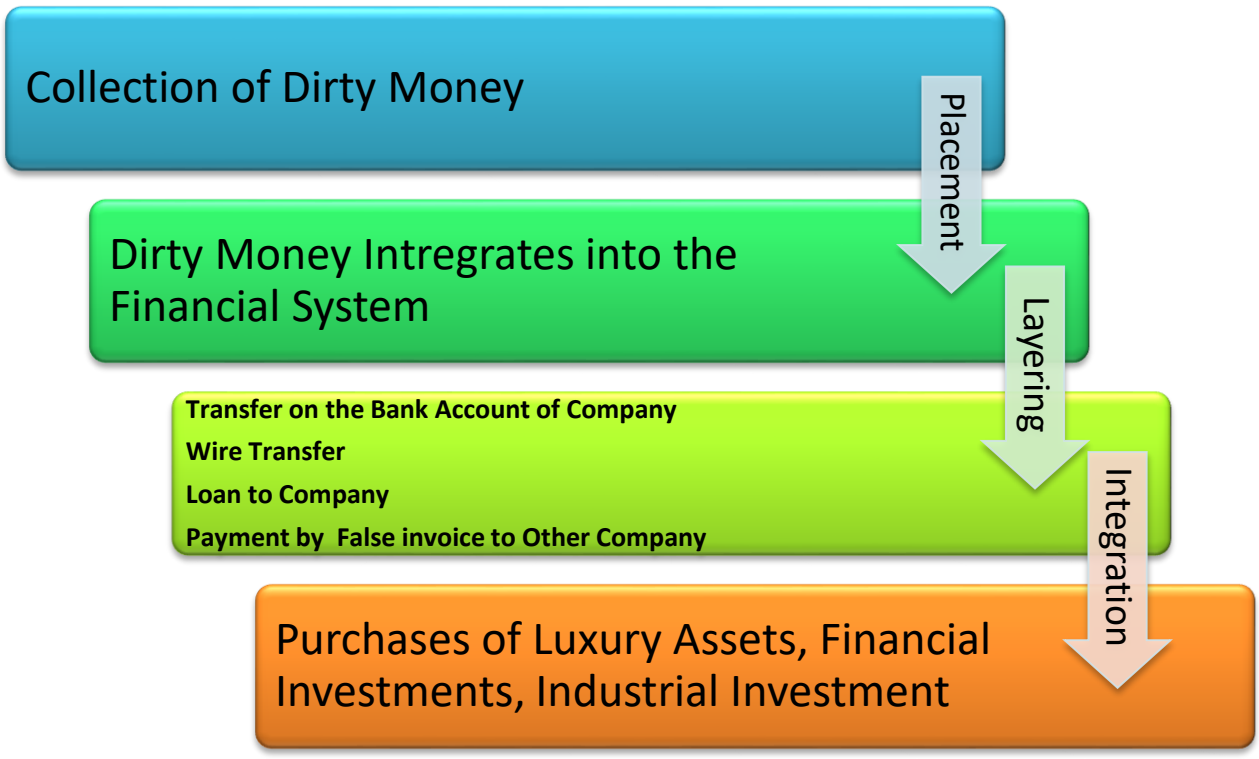
ii. A trail of money earned through illegal activities can become an evidence of crime. Criminals must conceal or disguise the source of their wealth to avoid prosecution.

iii. The proceeds from crime often become the target of investigation and seizure. To cover ill-gotten gains from suspicion and protect them from seizure, criminals must conceal their existence or alternatively, give them a legitimate look.

1.4 Money laundering process involves 3 steps:

Money laundering is not a single act but a process accomplished in 3 basic stages placement, layering and integration which may comprise numerous transactions by the launderers. A typical money laundering scheme is illustrated below:

Typical Money Laundering Scheme



Placement means the initial deposit of illegally derived funds either through its introduction into the financial system; through the purchase of high value goods; or by physical cross-border transportation.

Layering means a series of transactions or movement of funds with the aim of distancing them from their source. That is complex web of transactions to confuse the audit trail.

Integration means re-entry of funds into financial system appearing as normal business e.g. through investment in real estate, luxury assets or business. In short, the layered funds are brought back into the legitimate economy or legitimate use.

The three basic steps may occur as separate and distinct phases. They may also occur simultaneously or, more commonly, may overlap. Steps used depend on the available laundering mechanisms and the requirements of the criminal organizations.

Money laundering predicate offense is the underlying criminal activity that generated proceeds, which when laundered, results in the offense of money laundering. This includes:

a) corruption and bribery;
b) counterfeiting currency;
c) counterfeiting documents;
d) extortion;
e) fraud;
f) forgery;
g) breaking copy right/ intellectual right rules;
h) terrorism financing for terrorist activity;
i) Adulteration or breaking the copy right;
j) illicit arms trafficking;
k) illicit dealing in narcotic drugs and psychotropic substances;
l) illicit dealing in stolen and other goods;
m) kidnapping, illegal restraint, hostage-taking;
n) murder, grievous bodily injury;
o) woman and child trafficking;
p) smuggling;
q) smuggling and duty related crime;
r) unauthorized cross-border transfer of domestic and foreign currency;
s) robbery or theft;
t) trafficking in human beings and migrant smuggling;
u) sexual exploitation;
v) tax related crime;
w) insider trading & market manipulation;
x) organized crime;
y) financial benefit by means of threaten;
z) environmental crime;
aa) dowry and
bb) any other offence which Bangladesh Financial Intelligence Unit (BFIU) with the approval of the Government and by notification in the Official gazette declares as predicate offence for the purpose of this ordinance.

1.5 Combating Terrorist Financing (CTF)

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 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.

(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 b e deemed to have committed the offence of financing terrorist activities.

1.6 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.

1.7 Scope and Objective of the Policy

This policy is applicable for all sorts of products, operations and activities MFIL is operating in. In

branches/ subsidiaries, the Company would ensure compliance with the internal regulations on ML/ CTF or that of the Bangladesh Financial Intelligence Unit (BFIU) wherever are more exhaustive.

The objective of this policy is to ensure that MFIL has designed and implemented processes and procedures that are consistent with regulatory guidelines and the objectives and purposes of the ML/CTF Act.

The overall framework for ML and CTF regime in MFIL is designed so that the business units will take responsibility for:

- verifying the true identity of customers prior to providing the designated services (customer due diligence and Know Your Customer);
- reporting all suspicious transactions to Bangladesh Financial Intelligence Unit (BFIU);
- keeping appropriate records for the stipulated time as determined by Bangladesh Financial Intelligence Unit (BFIU);
- provide, from time to time, information as required by Bangladesh Financial Intelligence Unit (BFIU); and
- developing implementing and complying with all ML/CTF related regulatory requirements.

Chapter Two: Vulnerabilities for MFIL and their mitigation

Money launderer may use different financial products like lease, loans, and deposit scheme etc. to launder their money. Possible ways of laundering mechanism of ill money through use of MFIL"s products or services are discussed below.

2.1 VULNERABILITIES OF PRODUCTS AND SERVICES

a) Lease/Term Loan Finance

Money launderers and terrorist financer can use this instrument for placement and layering of their ill-gotten money.

Front company can take lease/term loan finance from MFIL and repay the loan from illegal source, and thus bring illegal money in the formal financial system in absence of proper measures. The company 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 MFIL's financing facility can be sold immediately after repayment of the loan through illegal money and sold proceeds can be shown as legal.

b) Factoring

MFIL introduced its Factoring financing recently considering its different market segment. Using its complex business mechanism, 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 MFIL and MFIL may get repayment from buyer. MFIL 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.

c) Personal Loan/Car Loan/Home Loan

Any person can take personal loan from MFIL 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.

d) SME/Women Entrepreneur Loan

Small, medium and women entrepreneurs can take loan facilities from MFIL 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.

e) Deposit Scheme

MFIL sell deposit products with at least a three months maturity period. The depositor may en-cash

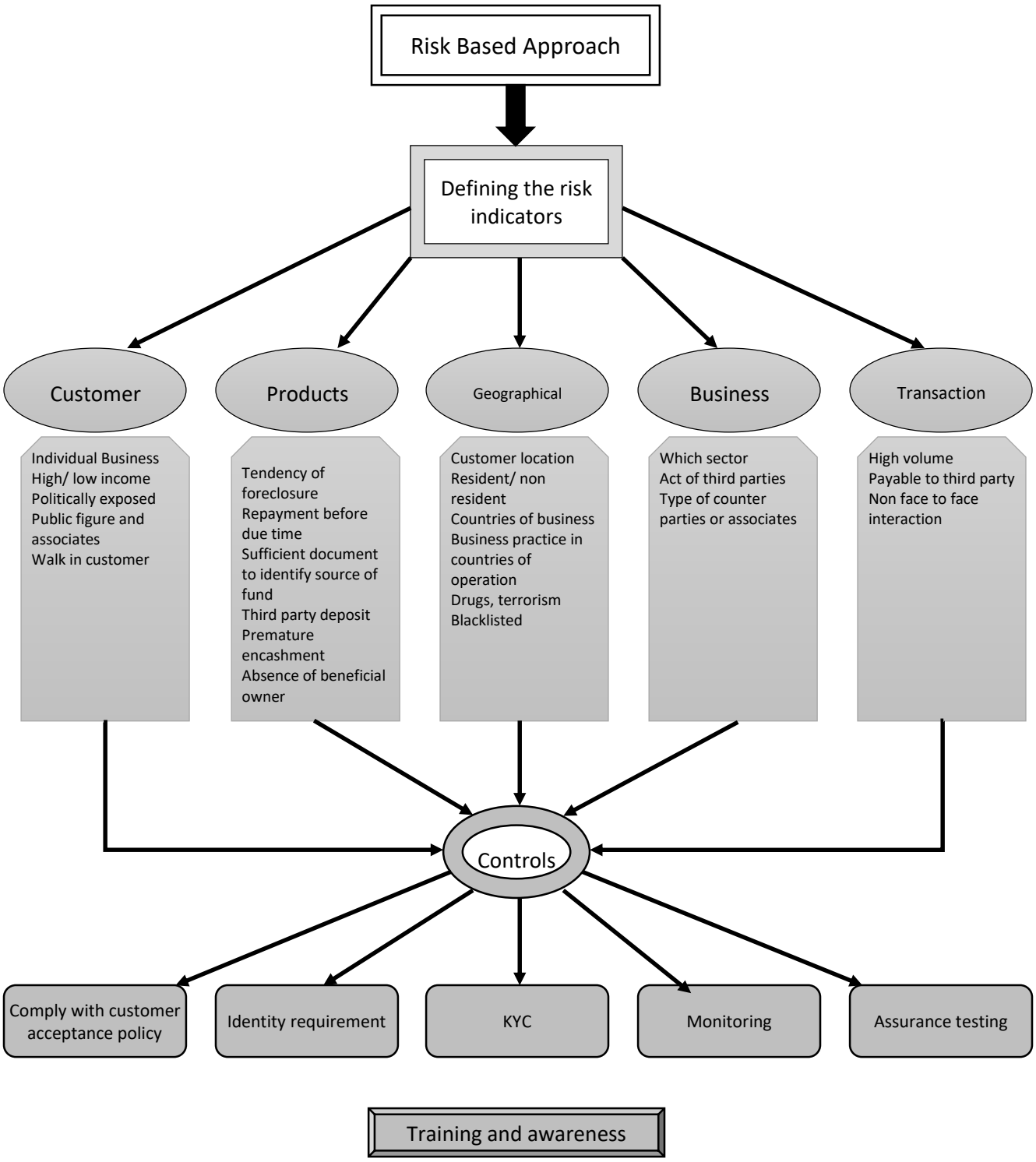
their deposit money prior to the maturity date with prior approval from Bangladesh Bank, foregoing interest income. This deposit product may be used as lucrative vehicle to place ill-gotten money in the financial system in absence of strong measures.

f) 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.

2.2 MITIGATION PROCESS

To mitigate the vulnerabilities an integrated risk based system should be followed to assess the relevant risk sectors and implement the appropriate risk based due diligence. A Risk Based control process should be as follows:



2.2.1 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 MFIL free from any such risk.

To protect MFIL from risks of money laundering or/and terrorist financing by customers willful or unwilling activities, we should strictly follow conduct Customer Due Diligence at different stages such as:

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

We have to ensure the following things to mitigate customer identity related risks:

- To be sure about the customer's identity and underlying purpose of establishing relationship with us, we will collect adequate information up to its satisfaction
- If a person operates an account on behalf of the customer, MFIL 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.
- 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.).
- 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.
- 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.
- While opening and/or operating account of Politically Exposed Persons (PEPs) enhanced due diligence shall have to be exercised. Following instructions shall have to be followed to ensure Enhanced Due Diligence (EDD). Detailed procedure of EDD is annexed in **Appendix** 2.

2.2.1.1 Non-Face to Face Contact:

Where there is no face-to-face contact, following procedure need to be followed:

- ✓ Photographic identification would clearly be inappropriate procedures to identify and authenticate the customer.
- ✓ FIs should ensure that there is sufficient evidence, either documentary or electronic, to confirm address and personal identity.
- ✓ At least one additional check should be undertaken 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.
- ✓ FIs should not allow non-face to face contact to a resident in establishing relationship.

2.2.2 Product vulnerabilities:

We have to identify and mitigate product-based vulnerabilities in the following ways:

- We have to be cautious regarding repayment before due time.
- We have to collect the sufficient document to identify the source of fund.
- Have to be cautious in terms of third party deposit.
- Premature encashment of deposit products.

2.2.3 Geographical vulnerabilities:

We have to identify and mitigate geographical vulnerabilities in the following ways:

- We have to be cautious about customer location and the customer's residential status.
- Understand the business practice in countries of operation.
- Careful about those countries those are famous in drugs and terrorist activities.
- Careful about border area's business activities.

2.2.4 Business vulnerabilities:

We have to identify and mitigate business vulnerabilities in the following ways:

- Which sector the customer operates its business.
- Complete and correct information from reliable sources to identity 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.

- Type of counter parties or associates.

2.2.5 Transaction vulnerabilities:

We have to identify and mitigate transaction vulnerabilities in the following ways:

- We have to be cautious on high volume transaction.
- No non face to face interaction is acceptable.

- Need extra cautious where customer request to pay to a third party.
- Careful about border area's business activities.

Chapter Three: COMPLIANCE PROGRAM

The compliance program should be documented, approved by the Board of Directors and communicated to all levels of the organization. As part of its ML/FT policy, CCU communicate clearly to all employees on annual basis through a statement from the Managing Director that clearly sets MFIL"s policy against money laundering and any activity which facilitates money laundering or the funding of terrorist or criminal activities.

3.1 CENTRAL COMPLIANCE UNIT

Central Compliance Unit (CCU) of MFIL will ensure the compliance of the Money Laundering Prevention Act. 2012 and Anti-Terrorism (Amendment) Act, 2013, and Bangladesh Financial Intelligence Unit (BFIU) regulations. Meridian Finance had already established Central Compliance Unit (CCU) in 2015.

3.1.1 Formation of CCU:

As per Bangladesh Financial Intelligence Unit (BFIU) Instructions, the CCU will be headed by a senior level employee whose position cannot be lower than the third rank in seniority in organizational hierarchy and a minimum of seven years of working experience, with a minimum of three years at a managerial level/ administrative level. The Head of CCU will also be considered as the CAMLCO of the Company. S/he will be assisted by Deputy CAMLCO & three other designated officers among which two will be from the general banking and information system department and none from the Internal Audit department. The organogram of CCU is shown below.

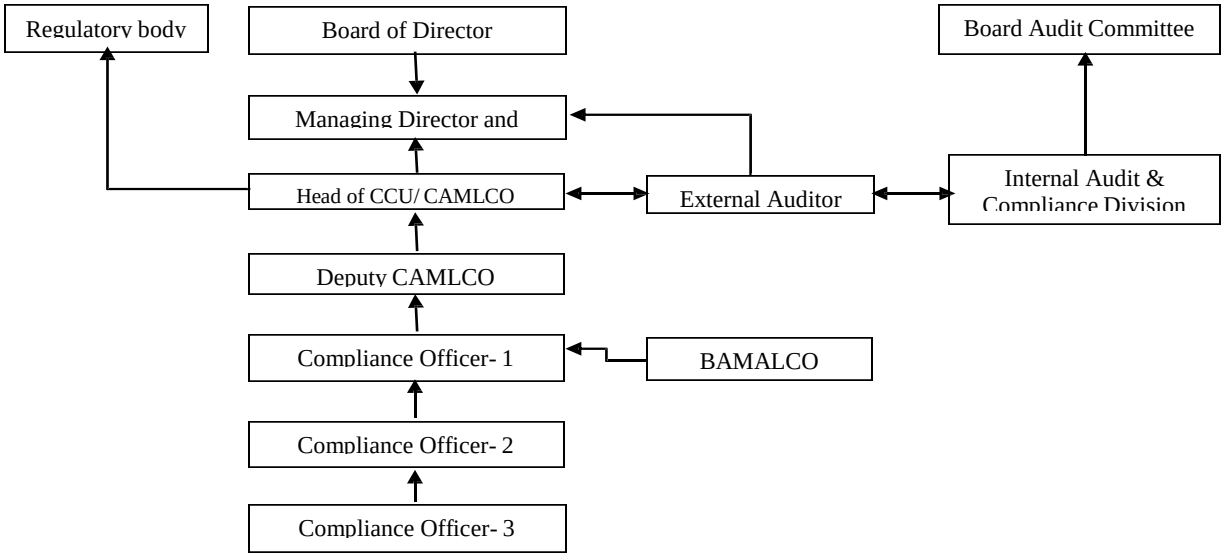


Fig: Formation of Central Compliance Unit

The designated CAMLCO/Head CCU should be a central point of contact for communicating with the regulatory and/or investigation agencies regarding issues related to financial institution's ML/FT program.

CCU will issue the instructions to be followed by the branches; these instructions will be prepared on the basis of combination of issues in monitoring of transactions, internal control, policies and procedures from the point of view of preventing money laundering & terrorist financing.

3.1.2 Departmental Duties/Responsibilities

The chain of duties and responsibilities at branches are as under:

Personnel	Duties/Responsibilities
Officer in charge of Accounts or vested with the authority to open new accounts	- To interview the potential customer - To verify the introductory reference/customer profile. - To arrive at threshold limit for each account (new as well as existing) and to exercise due diligence in identifying suspicious transactions. - To ensure non opening of accounts in the name of terrorist/banned organizations. - To adhere with the provisions of *Money Laundering Prevention Act 2012 and Anti-Terrorism Act 2013*. - To comply with the guidelines issued by Bangladesh Financial Intelligence Unit (BFIU) and by the company from time to time in respect of opening and conduct of account.
Chief Risk Officer	- To assess the money laundering and terrorist financing risk involve in the operating activities of the company evaluate the adequacy and effectiveness of the control set for safeguarding the company against such risks.
Head of Operations	- To scrutinize and ensure that the information furnished in the account opening form/customer profile/ threshold limit are in strict compliance with KYC guidelines before authorizing opening of account. - To certify regarding compliance with KYC guidelines and report suspicious transactions to CAMLCO/Managing Director.
Internal Auditor	- To verify and record his comments on the effectiveness of measures taken by the concerned officials and the level of implementation of KYC guidelines.
CAMLCO	- Implements and enforces Institution's anti-money laundering policies - Reports suspicious clients to Bangladesh Financial Intelligence Unit (BFIU) on Institution's behalf - Informs Controller of Branches of required actions (if any)

Top Management	- Prompt reporting of information regarding suspicious transactions to concerned law enforcing authority in consultation with Solicitors.

3.1.3 The responsibilities of a CCU shall include:

a) preparing an overall assessment report after evaluating the self-assessment reports received from the branches and submitting it with comments and recommendations to the chief executive of MFIL;

b) Preparing an assessment report on the basis of the submitted checklist of inspected branches by the Internal Audit Department on that particular quarter;

c) Submitting a half-yearly report to BFIU within 60 days after end of a quarter.

3.1.3.1 Responsibilities of CAMLCO:

The Chief ML/FT Compliance Officer may choose to delegate duties or rely on suitably qualified Employee for their practical performance whilst remaining responsible and accountable for the operation of the designated functions. The major responsibilities of a CAMLCO are as follows:

1) To implement and enforce corporate-wide ML/FT policies, procedures and measures. The CAMLCO will directly report to the Managing Director for his responsibility. The CAMLCO shall also be responsible to coordinate and monitor day to day compliance with applicable ML/FT related laws, rules and regulations as well as with its internal policies, practices, procedures and controls.

2) To monitor, review and coordinate application and enforcement of the MFIL compliance policies including ML/FT Compliance Policy. This will include - an ML/FT 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 ML/FT training plan.

3) To monitor changes of laws/regulations and directives of Bangladesh Financial Intelligence Unit (BFIU) and revise MFILs internal policies accordingly;

4) To respond to compliance questions and concerns of the Employee and advise branches assist in providing solutions to potential issues involving compliance and risk;

5) To ensure that the MFILs ML/FT 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;

6) To develop the compliance knowledge of all Employee, especially the compliance personnel and conduct training courses;

7) To develop and maintain ongoing relationships with regulatory authorities, external and internal auditors, branch/unit heads and compliance resources to assist in early identification of compliance issues;

8) To assist in review of control procedures to ensure legal and regulatory compliance and in the development of adequate and sufficient testing procedures to prevent and detect compliance lapses;

9) To monitor the business through self-testing for ML/FT compliance and take any required corrective action;

10) To manage the STR/SAR process:

- reviewing transactions referred by branch compliance officers as suspicious;
- reviewing the transaction monitoring reports;
- ensuring that internal Suspicious Activity Reports (SARs):

a) are prepared when appropriate;

b) To reflect the uniform standard for ―suspicious activity involving possible money laundering or terrorist financing‖ established in MFILs policy;

c) are accompanied by documentation of the branches decision to retain or terminate the account as required under MFILs policy;

d) are advised to other branches who are known to have a relationship with the customer;

e) are reported to the Managing Director when the suspicious activity is judged to represent significant risk to MFILs 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;

3.1.3.2 Responsibilities of Deputy CAMLCO:

The major responsibilities of a Deputy CAMLCO are as follows:

- Assisting CAMLCO in implementing and enforcing Institution's anti-money laundering policies.
- Monitor reports regarding suspicious clients to Bangladesh Financial Intelligence Unit (BFIU) on Institution's behalf.
- Controlling flow of information to BMLCO for required actions (if any)

3.2 BRANCH ANTI-MONEY LAUNDERING COMPLIANCE OFFICER

There has to be a Branch Anti-Money Laundering Compliance Officer (BMLCO) at each branch. Branch Manager shall be the BMLCO. The responsibilities of a BMLCO are as follows:

- Manage the transaction monitoring process
- Report any suspicious activity to CCU
- Provide training to Branch Employee
- Communicate to all Employee in case of any changes in national or its own policy
- Submit branch returns to CAMLCO timely.

3.3 EMPLOYEE TRAINING AND AWARENESS PROGRAM

To ensure the proper compliance of anti-money laundering and combating terrorist financing activities a robust training program have to be in place. Employees in different business functions need to understand policy, procedures, and controls affect them in their day to day activities. MFIL shall arrange yearly (for General Training) or half yearly (for Job Specific and New Joiner's) training program to ensure proper compliance of money laundering and terrorist financing prevention activities. Following training procedures to be followed by the Company for prevention of Money Laundering and Terrorist Financing activities:

3.3.1 Employee Awareness

Employee 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 employees must be trained to co-operate fully and to provide a prompt report of any suspicious transactions/activities.

3.3.2 Education and Training Programs

All relevant Employees 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 Employee should be alert to any change in the pattern of a customer's transactions or circumstances that might constitute criminal activity.

Generally, all trainings could be divided in to two types:

a. General training
b. Job Specific Training

(a) General Training

A general training program has to be organized on a yearly basis, which include the following:

- General information on the risks of money laundering and terrorist financing schemes, methodologies, and typologies.
- Legal framework, how ML/FT related laws apply to MFIL.
- 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.

(b) Job Specific Training

- **New Employee Training**

For a new employee the compliance policy statement must be sign-off at the beginning of the joining and he/she must have a on the job training from the departmental head regarding the importance of money laundering and terrorist financing activities. The respective new employee must go through the yearly training on ML/CTF.

- **Customer Service/Relationship Managers**

Retail and investment departments employee 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.

- **Operation Department**

Operation department employee who received completed Account Opening, FDR, DPS related application forms and cheques for deposit into customer's account or other investments must receive training in the processing and verification procedures. 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. Employee should be aware that the offer of suspicious funds or the request to undertake a suspicious transaction may need to be reported to the ML/FT 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.

- **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.

- **Audit and compliance officer**

Internal auditors are charged with overseeing, monitoring and testing ML/FT controls, and they should be trained about changes in regulation, money laundering and terrorist financing methods and enforcement, and their impact on the institution.

- **Senior Management Commitment and role of the Board of Directors**

The most important element of a successful ML/CTF program is the commitment of senior management, including the Managing Director/managing director and the board of directors. Money laundering and terrorist financing issues must be communicated to the board. An anti-money laundering compliance report should be submitted in each board meeting. The message from top management and the board of directors will be "Zero Tolerance" in case of money laundering and terrorist financing

- **ML/FT Compliance Officer**

The ML/FT Compliance Officer should receive in depth training on all aspects of the Money Laundering and Terrorist Financing Prevention Legislation, Bangladesh Financial Intelligence Unit (BFIU) directives and internal policies. In addition, the ML/FT 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.

3.3.3 Training and Awareness Procedures for Trainers

The trainers to be followed the below 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. 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.
- 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.

3.4 SUSPICIOUS TRANSACTION REPORTING (STR)

According to the provision of section 25 (1) (d) of MLPA, 2012, the MFIL should report to BFIU proactively and immediately, facts on suspicious, unusual or doubtful transactions likely to be related to money laundering. Because BFIU has the power to call STR from FIs related to financing of terrorism according to section 15(a) of Anti-terrorism (Amendment) Act, 2012.

3.5 SELF ASSESSMENT PROCEDURE

Self-Assessment is a procedure performed by the ML compliance officer to assess how effectively ML/FT program is going on around the company. Such procedure must be carried on a half yearly basis. This procedure enables management to identify areas of risk or to assess the need for additional control mechanisms.

The self-assessment should conclude with a report documenting the work performed, how it was controlled/ supervised and the resulting findings, conclusions and recommendations. The self-assessment should advise management whether the internal procedures and statutory obligations of MFIL have been properly discharged.

Each branch will assess its ML/FT activities on a half yearly basis and submit the report to the CCU within next 20 days. However, self-assessment will be done on the following areas:

- The percentage of officers/employees that received official training on ML/FT;
- The awareness of the officers/employees about the internal ML/FT policies, procedures and programs, and Bangladesh Financial Intelligence Unit (BFIU) instructions and guidelines;

- The arrangement of ML/FT 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;
- Identification of Suspicious Transaction Reports (STRs);
- The maintenance of a separate file containing MLPA, Circulars, Training Records, Reports and other ML related documents and distribution of those among all employees;
- The measures taken by the branch during opening of account of PEPs/IPs;
- Consideration of UN Sanction List while conducting any business.
- The compliance with ML/FT weaknesses/irregularities, as the bank's Head Office and Bangladesh Financial Intelligence Unit (BFIU) inspection report mentioned.

A standard checklist for self-assessment as advised by Bangladesh Financial Intelligence Unit (BFIU) has been attached in Annexure.

3.6 INDEPENDENT TESTING PROCEDURE

The Internal Audit and Compliance team of MFIL shall perform at least annually an independent testing on the adequacy of ML controls across the organization. Results of independent testing procedure should be communicated to the Board Audit Committee. The Board may appoint external auditors to perform independent testing procedures each year to review the adequacy of controls if require or statutory auditors may review the internal control and reporting process of ML/FT of the Company within the scope of their appointment. Both Internal Audit and External Audit should focus their audit program on risk factors and conducts intensive reviews of higher risk areas where controls may be deficient.

Such independent testing will cover the following areas:

- Branch Compliance Unit/BMLCO ML procedure
- Knowledge of officers/employees on ML/FT issues
- Customer Identification (KYC) process
- Know your employee (KYE) 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 ML 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 MFIL"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 MFIL management; 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.

A standard checklist for independent testing procedure as advised by Bangladesh Financial Intelligence Unit (BFIU) has been attached in Annexure.

3.7 Independent Audit Function

Independent audit function is very important to ensure the effectiveness of ML/FT program. Auditors should act independently and report directly to the Board of Directors if there is any breach of policy and procedures. Auditor's responsibilities regarding compliances are as follows:

3.7.1 Internal audit

The responsibilities of internal auditors are:

- Address the adequacy of ML/FT 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.
- Perform appropriate transaction testing with particular emphasis on high risk operations (products, service, customers and geographic locations).
- Assess the adequacy of the MFIL processes for identifying and reporting suspicious activity.
- Communicate the findings to the board and/or senior management in a timely manner.
- Track previously identified deficiencies and ensures that management corrects them.
- Assess training adequacy, including its comprehensiveness, accuracy of materials, training schedule and attendance tracking.
- Employee accountability for ensuring ML/FT compliance.
- Comprehensiveness of training, in view of specific risks of individual business lines.
- Participation of personnel from all applicable areas of the Company.

- Coverage of different forms of money laundering and terrorist financing as they relate to identifying suspicious activity.

- Penalties for noncompliance and regulatory requirements.

3.7.2 External Auditor

MFIL may, if requires, facilitate the external auditors in reviewing whether the ML policies have been complied or not by the management.

Chapter Four: Customer Due Diligence (CDD)

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 ML/FT efforts, and is the most effective defense against being used to launder the proceeds of crime.

4.1 KNOW YOUR CUSTOMER (KYC) PROCEDURE

Where MFIL 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.

The following points should be taken care of in this regard

- **Nature of Customer's Business**
  When a business relationship is being established, the nature of the business that the customer expects to conduct with MFIL 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.

- **Identifying Real Person**
  The prospective customer should be interviewed personally. This will safeguard against opening of fictitious account. Face to face communication is must.

- **Document is not enough**
  The best identification documents possible should be obtained from the prospective c u s t o m e r i.e. those that are the most difficult to obtain illicitly.

- **Reliance on Third party**
  For the use of third party following criteria should be meet:

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

  (b) (b) MFIL 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) We should satisfy ourselves that the third party is regulated, supervised or monitored for, and has measures in place for compliance with, CDD and record-keeping

requirements.

4.2 COMPONENTS OF KYC PROGRAM

KYC should be the core feature of MFIL‟s risk management and control procedure and be complemented by regular compliance reviews and audit.

Essential elements should start from the risk management and control procedures and should include-

a. Customer acceptance policy
b. Customer identification
c. Ongoing monitoring of high risk accounts, and
d. Identification of suspicious transactions

4.2.1 Customer acceptance policy,

Selection of Customer is an important factor for Banks and NBFIs. Meridian Finance & Investment Limited (hereinafter read as MFIL) takes into consideration of all the relevant factors for accepting customers like- Customer's background, business/personal activities, business risks, credit worthiness, political influence, social status, other basic information and risk factors.

On the other hand to combat risk of Money Laundering (ML) and Financing of Terrorism (TF) Know Your Customer (KYC) and Customer Due Diligence (CDD) are important tools. Lack of precaution in the above mentioned factors might result in serious customer and counterparty risks, especially reputation, operational, legal and compliance risks. Collection of sufficient information about the customers is the most effective defense for combating ML/TF activities. As per Money Laundering Prevention Act (MLPA)-2012 each financial institution (FI) is required to keep satisfactory evidence of the clients. On the other hand, each FI is also required to make necessary arrangement to prevent transactions related to crimes as described in Anti-Terrorism Act (ATA)-2009 (as amended up to 2013). It also requires to identify, under these laws, suspicious transactions with due care and diligence. Pursuant to the above legal bindings, Guidance Notes issued by Bangladesh Financial Intelligence Unit (BFIU) on ML/TF and Global standards, MFIL has developed the Customer Acceptance Policy as under:

1) MFIL will comply all the prevailing regulations of MLPA-2012 and ATA-2009 (to be amended from time to time) and Bangladesh Financial Intelligence Unit (BFIU) Guidelines relating to establishing financial relationship with customers.

2) Documentation requirements and other information shall be collected in compliance with the instructions contained in BFIU Circular#02 dated July 17, 2002; the requirements of the MLPA-2012 and ATA-2009 and other circulars and guidelines issued/ to be issued by Bangladesh Financial Intelligence Unit (BFIU) from time to time.

3) MFIL will not open or maintain any account or establish any financial relationship with person(s) or organization(s) convicted for terrorism or terrorist financing or listed on the United Nations Security Council Resolution (UNSCR) 1267 & 1373-as individual, entities, alliances - terrorist or terrorist organizations.

4) In case of opening account of a Politically Exposed Person (PEP), MFIL will comply the instructions contained in BFIU Circular#14 dated September 25, 2007 issued by Bangladesh Financial Intelligence Unit (BFIU). Such types of account will be classified as high risk and will require very high level of monitoring. PEPs account shall be opened with prior permission of the Managing Director.

5) At the time of opening new account MFIL will take care to seek only such information from the customer which is relevant but not intrusive. As customers profile and information contained therein are confidential documents, those should not be divulged for any other purposes.

6) MFIL will conduct necessary checks before opening a new account so as to ensure that the name of the customers do not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations etc. as declared by the Government authorities.

7) MFIL will collect complete and correct information of identity of the beneficial owners and preserve in the concerned file. A person shall be treated as a beneficial owner if (i) he or she has controlling share of a company or and (ii) hold 20% or more share of a company.

8) MFIL will, in case a customer operate an account on behalf of another person in his/her own name, collect complete and correct information of the person besides the account holders.

9) MFIL will ensure certification/genuineness of the given documents/National ID/Social Security Number/Residence Permit/TIN, independent contact with the customer etc. in case of establishing business relationship with "Non-Face to Face Customer/Non-resident Bangladeshi"

10) MFIL will review the customer's personal/business background with due diligence before establishing any financial relationship.

11) MFIL, in no cases, will allow any anonymous or fictitious accounts to be opened/ to be continued.

12) Customers' risk shall be assessed as defined in KYC Profile meticulously and shall review the same at least once in a year or at the time of renewal or providing loan against FDR or new sanction or any other business relationship.

13) MFIL will accept only those customers who can provide documents relating to identity and physical existence of business or residence.

14) The Branches shall not open any account, where MFIL is unable to apply appropriate customer due diligence measures but the branch must be careful to avoid unnecessary harassment of the customer.

15) MFIL will verify identity of the customers using reliable sources, documents etc. but it must retain copies of all references, documents used to verify the identity of the customers.

16) MFIL will comply Uniform Account Opening Form with prescribed KYC at the time of completing account opening formalities as per BFIU Circular Letter#02 dated: March 15, 2015.

17) MFIL will take necessary steps to close existing accounts, where necessary, due to non-cooperation of the customers in providing necessary documents/information required by law/regulatory authority or non-reliability of the information/documents furnished by them. Decision to close an account shall be subject to approval of the Managing Director.

18) MFIL will not do anything that will cause inconvenience to the general public, especially those who are financially or socially disadvantaged.

19) MFIL, in no cases, will deal with any Shell company or Shell bank.

20) MFIL reserves the right to discontinue or close relationship, which in its opinion has contravened the MLPA-2012 and ATA-2009, and any other laws of the Country or indicates suspicious transaction/business.

4.2.2 Monitoring of high risk accounts, and identification of suspicious transactions.

High value single transaction conducted in a single Demand Draft, Pay Order, Transfer by any person or institution or any person/institution involved in a financial transaction that may pose reputational and other risks to MFIL. In this case if a transaction appears abnormal in relation to the usual transaction of the concerned person or institution that transaction will be treated as ―high value and suspicious.

4.2.3 Customer Identification

According to the ML Circular No. 24 dated 03/03/2010, for the purpose of KYC Procedure a "Customer" is means:

- any person or institution maintaining an account of any type with a MFIL;
- the person or institution as true beneficial owner in whose favor 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;

4.2.3.1 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 Registration, Passport/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. It 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.

4.2.3.2 KYC for Individual Customers

MFIL 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 number.

Relationship Officer of MFIL should always bear in mind the following points:

1) MFIL will not allow non-face to face contact to any business relationship.
2) Particular care should be taken in accepting documents which are easily forged or which can be easily obtained using false identities.
3) In respect of joint accounts where the surname and/or address of the account holders differ, the name and address of all account holders should be verified.
4) Any subsequent change to the customer's name, address, or employment details of which the MFIL becomes aware should be recorded as part of the Know Your Customer process.
5) All documents collected for establishing relationship must be filed in with supporting evidence. Where this is not possible, the relevant details should be recorded on the applicant's file.
6) 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.
7) In the case of socially or financially disadvantaged people such as the elderly, the disabled, students and minors, the identity of these persons can be verified from an original or certified copy of alternative document, preferably one with a photograph. Certificate or confirmation from lawyer, accountant, director or manager of a regulated institution, a notary public, a member of the judiciary or a senior civil servant is acceptable to MFIL in this regard. The Certifier must sign the copy document and clearly indicate his position or capacity on it with a contact address and phone number. However, MFIL shall not allow "high value" transactions to this kind of customers.
8) The normal identification procedures set out above should be followed. Moreover, in case of minor parents/ legal guardians KYC procedure must be followed.
9) Identification documents which do not bear photographs or signatures are not acceptable. More importantly checking of authenticity of the identity documents is must.
10) To verify the customer permanent and present address Passport/ NID and recent utility bill's

copy can be checked.

11) The original, certified copy of (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 should be used to identify the customer:

4.3 Business segment wise KYC requirements

4.3.1 KYC for Corporate Bodies and Other Entities

The principal requirement for the corporate bodies is to verify its legal existence and to look who is actually behind the 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.

The following documents should 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 Schedule X and Form XII.

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 (listed in any exchanges) 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, identities of all current signatories should be taken and have to verify.

4.3.2 KYC for 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 is particularly 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.

4.3.3 KYC for Partnerships and Unlisted Businesses

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

4.3.4 Powers of Attorney/ Mandates to Operate Accounts

Establish the identities of holders of powers of attorney, the grantor of the power of attorney. Records of all transactions undertaken in accordance with a power of attorney should be kept.

4.3.5 Transaction Monitoring Process

The nature of this monitoring will depend on the nature of the business. The purpose of this monitoring is for Financial Institutions to be vigilant for any significant changes or inconsistencies in the pattern of transactions.

Possible areas to monitor could be: -

- transaction type
- frequency
- unusually large amounts

- geographical origin/destination
- changes in account signatories

Loan/ Credit transactions:

- Customer uses cash collateral to obtain loan/facility.
- End use of loan proceeds not consistent with purpose.
- Borrower settling "problem" loans by large amounts of cash suddenly with no reasonable explanation of funds/source.
- Purpose of loan does not make economic sense; or provision of cash collateral.
- Using cash deposit for collateralizing a loan.
- Loan proceeds unexpectedly channeled offshore.

4.3.6 Duties if Customer Due Diligence (CDD) cannot be performed

If completion of CDD cannot be performed due to uncooperative nature of the client and/or if the information provided is found to be incredible after assessment, FI may take into the following actions:

1. Bank/FI may not open account of such client or may close the account if appropriate.
2. Before closure of such accounts, approval from top management is necessary and the account holder must be informed via notice detailing the reason behind such closure of account.

Suspicious Transaction (STR) may be reported on case to case basis in this regard.

A standard KYC Template Attached in **Appendix # 3 & 4.**

4.4 Steps for combating with terrorist financing by MFIL:

To prevent the possibility of borrowing customers to undertake such activities as money laundering and channelizing of loan funds for terrorist financing, it is important to undergo detailed profiling of the borrowing customer to identify the owners, understand their business and thereby form a fact- based opinion on them.

The following steps will form the core component for the selection of the borrower who in MFIL‟s opinion may be considered as safe for conducting business:

1. Performing extensive Know Your Customer (KYC) exercise on the prospective client. The legal status of the legal person / entity will be verified through proper and relevant documents. This will include Trade License / Partnership Deeds / Memorandum and Articles of Association according to the constitution of the firm, along with copies of the list / register of directors. Satisfactory evidence of the identity of each of the principal beneficial owners being all directors of limited companies along with any owner holding 10% interest or more or with principal control over the company's assets will be obtained.

2. Appraisal of the credit proposal will involve extensive person to person contact betweenMFIL officials and customer's representatives, physical visits to the business premises, enquiries within the trade circles and with related trade parties in the peer group etc. A detailed understanding of the business activity proposed to be financed will be made from the above exercise. If any negative opinion is formed through this exercise or resistance is faced in collecting adequate information or access to business premises, the relationship will not proceed any further.

At the disbursement stage, the control will be made by ensuring that all disbursements are made by account payee cheques to confirm that the intended beneficiary of the financing is indeed the recipient of the fund. All loans are disbursed for specific terms either as lease financing, short term facilities or term loans. In case of lease financing, the beneficiary of the disbursement cheque will be the vendor of the goods to be procured. In the other cases, payment will have to be made to the customer.

As a deterrent to diversification of funds, the following undertaking will be included in the Letter of Agreement which is executed between the MFIL and the borrower at the time of availing the credit facilities:

"The borrower shall apply the proceeds of the loan exclusively for the purpose of the Project as set out in (Section number of the Agreement). Furthermore, the borrower undertakes not to apply the proceeds of the loan, either directly or indirectly, for carrying out any activities, including terrorist activities, which are prejudicial to the wellbeing of the state, in any form whatsoever."

4.5 KNOW YOUR EMPLOYEE (KYE)

Know Your Employee (KYE) program means the process 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.

HR department is to ensure the compliance of proper KYE procedure, background screening of prospective and current employees including criminal history. Only obtaining the related documents is not enough to ensure this compliance, authenticity of the documents must be ensured at the time of appointment of the employee(s).

A Standard KYE Template is attached in A**ppendix - 07**

Chapter Five: Suspicious Transaction Report (STR)/Suspicious Activity Report (SAR)

5.1 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 MFIL to the competent authorities.

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 ML/TF Act, any other transaction or attempt of transaction delineated in the instructions issued by Bangladesh Financial Intelligence Unit (BFIU) from time to time.

5.2 Identification and Evaluation of STR/SAR:

The identification and evaluation process of STR/SAR includes the following:

5.2.1. Identification STR/SAR

Generally the detection of unusual transactions/activities may something is 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.

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.

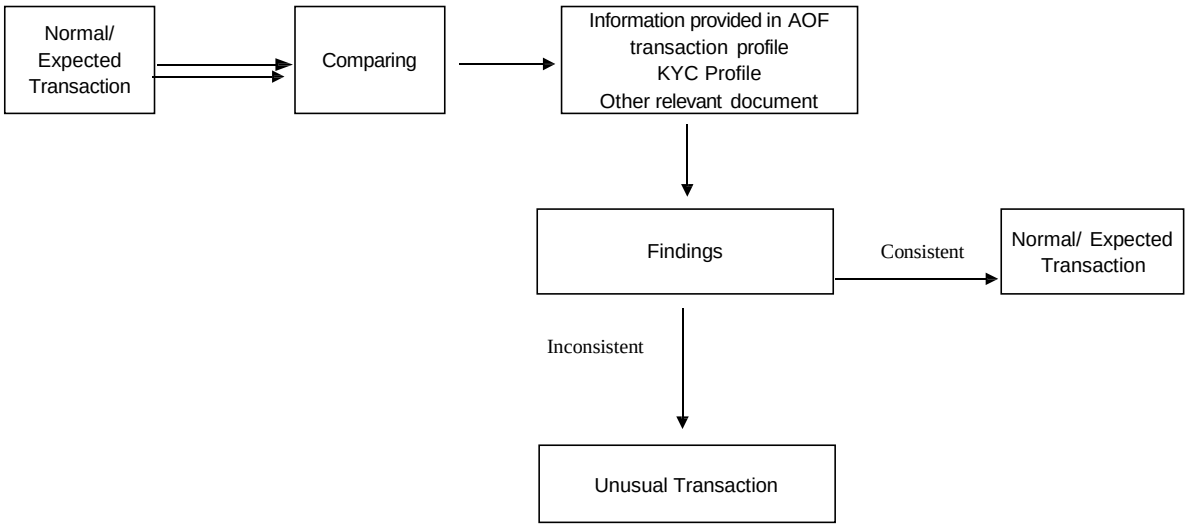


Fig: STR identification Process

5.2.2. Evaluation and Disclosure

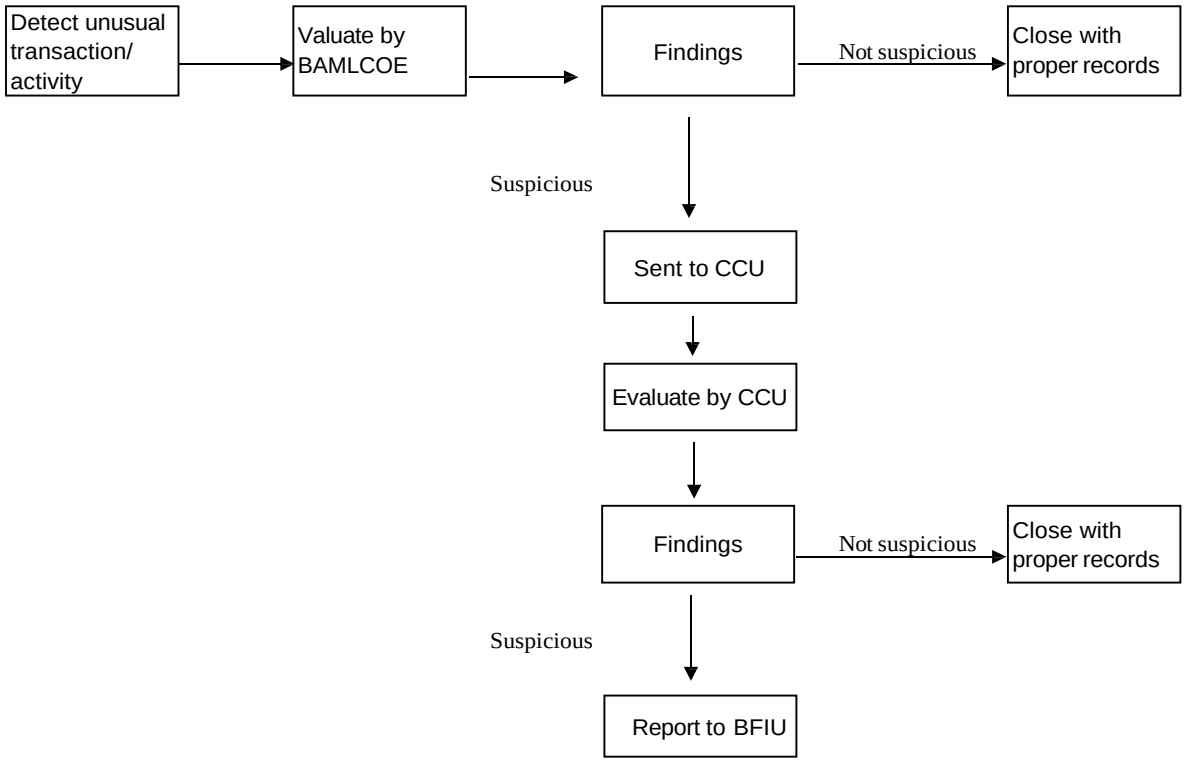
These problems must be in place at branch level and Central Compliance Unit (CCU). After identification of STR/SAR, at branch level BMLCO should evaluate the transaction/activity to identify suspicion by interviewing the customer or through any other means. In evaluation stage concerned BMLCO must be tactful considering the tipping off provision of the acts. If BMLCO 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 Financial Intelligence Unit or not) MFIL should keep records with proper manner.

At the final stage we should submit STR/SAR to Bangladesh Financial Intelligence Unit (BFIU) if it is still suspicious.

6.3 REPORTING OF STR/SAR

As per the MLPA, 2012 and ATA, 2009 (as amended in 2013) MFIL is obligated to submit STR/SAR to Bangladesh Financial Intelligence Unit. Such report must come to the Bangladesh Financial Intelligence Unit from CCU. As per the STR format specified by Bangladesh Financial Intelligence Unit (BFIU).

STR reporting procedure is described below:



Figs: STR Reporting Process

5.4 TIPPING OFF

Tipping off‟ means to disclose to the concern person regarding the reporting/investigation process. The offence of 'tipping off' occurs when information or any other matter which might prejudice the investigation is disclosed to the suspect of the investigation (or anyone else) by someone who knows or suspects (or, in the case of terrorism, has reasonable cause to suspect) that: an investigation into money laundering has begun or is about to begin, or the police/investigating authority have been informed of suspicious activities, or a disclosure has been made to another employee under internal reporting procedures.

As per section 6 of MLPA 2012 and FATF Recommendation 21 prohibits MFIL, 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 MFIL is seeking to perform its CDD obligation in those circumstances.

5.4.1 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.

5.5 INDICATORS OF STR

Moving Customers:
A customers who moves every month, particularly if there is nothing in that person's information suggesting that frequent changes in residence is normal, could be suspicious.

Out of market windfalls:

If you think a customer who just appeared at your institution sounds too good to be true, you might be right. Pay attention to one whose address is far from your institution, especially if there is no special reason why you were given the business. Aren't there institutions closer to home that could provide the service?

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 interest 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.

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 MFIL 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.

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.

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.

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.

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.

Suspicious Employee Activity:

- Employee exaggerates the credentials, background or financial ability and resources of a customer in written reports 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.

Other Suspicious Activity

Suspicious transaction basically means a transaction which is unusual or a transaction which we know or reason to believe that the proceeds came from illegal activities, a transaction may be suspicious in various ways, some insights of suspicious transaction but not limited may be as follows:

- 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.
- Gaps in critical information.
- Attempt to conceal information.

- Unnecessarily complex structure of transaction.
- Excessive request for secrecy of information.
- Unnecessary use of intermediaries.
- Doubtful beneficiary of the fund.
- A transaction which we know or reason to believe is unusual for the type of business the customer is in-has no business or apparent lawful purpose.
- Structuring of transaction to evade record keeping or reporting requirements.
- Loan transaction or credit facilities with inherently risky collateral or geographical characteristics.
- Unusual fund transfer from border areas.
- Inherently risky industries or geographical areas.

Chapter Six: Record Keeping

MFIL should maintain all necessary records on transactions for a period of at least five years as specified by the Guidance Notes issued by Bangladesh Financial Intelligence Unit or for such periods as specified by MFIL's documents retention policy (whichever is higher). This will enable the Company 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 MFIL on its customer relationship and transactions should be such that:

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

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 or for such periods as specified in MFIL"s

Documentation Retention Policy (whichever is higher) from the date when the relationship with the customer has ended. This is the date of:

(1) Closing of an account
(2) Providing of any financial services
(3) Carrying out of the one-off transaction, or the last in a series of linked one-off transactions; or
(4) Ending of the business relationship; or
(5) Commencement of proceedings to recover debts payable on insolvency.

6.1 RETRIEVAL OF RECORDS

The relevant records of the clients must be maintained in a systematic manner as prescribed in the record retention policy of the Company thus may retrieve easily and provide the customer's information or customer's transaction record without any delay for the requirement of regulatory body, law enforcing authority or for the purpose of internal use.

6.2 STR AND INVESTIGATION

We should not destroy any STR related records of customer or transaction without the consent of the BFIU even though the fifteen-year limit may have been elapsed. A register have to be maintain for all STR records, investigations and inspection made by the investigating authority 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.

6.3 TRAINING RECORDS

MFIL shall maintain training records which include:-

(i) details of the content of the training programs provided;
(ii) the names of Employee who have received the training;
(iii) the date/duration of training;
(iv) the results of any testing carried out to measure Employees understanding of the requirements; and
(v) an on-going training plan.

6.4 BRANCH LEVEL RECORD KEEPING

Branch has to ensure to keep the following records at the branch level in the form of shadow hard

copy.

(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, and
(7) Information provided to the Head Office or competent authority.

Chapter Seven: Statement of Compliance

MFIL should obtain a Statement of Compliance with Prevention of Money Laundering and Terrorist Financing from its all employees. Such statement of compliance should be dully signed by the respective employee and should be preserved in the employees‟ personal files.

In the Statement of compliance, every employee should solemnly declare and confirm that as an employee of MFIL I should:

1. Comply with applicable laws and regulations and corporate ethical standards.

2. Compliant with all rules and regulations in the normal course of my assignments. It is the responsibility of me to become familiar with the rules and regulations that relate to my assignment. Ignorance of the rules and regulations cannot be an excuse for non-compliance.

3. Be held accountable for carrying out their compliance responsibilities on ML/TF issues.

The CAMLCO should ensure that all new employees of the Company shall read this policy, understand the implications there of and signs the “Statement of Compliance”. After signoff, it should be sent to HR for maintain in his/her personal file.

Chapter Eight: Confidentiality of Information

All information generated, exchanged or provided with any personnel of the Company in the context of Anti Money Laundering/ Combating Terrorist Financing must be subjected to strict controls and safeguards to ensure that the information is used only in an authorized manner, consistent with provisions on privacy and data protection, where applicable.

Under MLPA 2012 and ATA 2013, MFIL or its employees‟ shall not share account related information to investigating authority i.e., Anti-Corruption Commission (ACC) or person authorized by ACC to investigate the said cases without having court order or prior approval from Bangladesh

Besides, section 6 of MLPA 2012 and FATF Recommendation 21 prohibits MFIL, 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 MFIL is seeking to perform its CDD obligation in those circumstances. 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.

Chapter Nine: Offences and Punishments

Penalties for non-compliance of Money Laundering Prevention Act 2012

According to section 25 (2) of MLPA, 2012, if any reporting organization violates the directions mentioned in sub-section (1) of section 25 of MLPA, 2012, Bangladesh Financial Intelligence Unit (BFIU) may-

(a) impose a fine of at least taka 50 (fifty) thousand but not exceeding taka 25 (twenty five) lacs on the reporting organization; and

(b) in addition to the fine mentioned in clause (a), cancel the license or the authorization for carrying out commercial activities of the said organization or any of its branches 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 the organization.

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

(a) If any reporting organization fails to provide with the requested information timely under this section, Bangladesh Financial Intelligence Unit (BFIU) may impose a fine on such organization which may extend to a maximum of Taka 5 (five) lacs at the rate of Taka 10 (ten) thousand per day and if any organization is fined more than 3(three) times in 1(one) financial year, Bangladesh Financial Intelligence Unit may suspend the registration or license of the organization or any of its branches 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 against the organization.

(b) If any reporting organization provides with false information or statement requested under this section, Bangladesh Financial Intelligence Unit may impose a fine on such organization not less than Taka 20 (twenty) thousand but not exceeding Taka 5 (five) lacs and if any organization is fined more than 3(three) times in 1(one) financial year, Bangladesh Financial Intelligence Unit (BFIU) may suspend the registration or license of the organization or any of its branches 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 against the said organization.

(c) If any reporting organization fails to comply with any instruction given by Bangladesh Financial Intelligence Unit under this Act, Bangladesh Financial Intelligence Unit may impose a fine on such organization 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 any organization is fined more than 3(three) times in 1(one) financial year, Bangladesh Financial Intelligence Unit may suspend the registration or license of the organization or any of its branches 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 against the said organization.

(d) If any reporting organization fails to comply with any order for freezing or suspension of transaction issued by Bangladesh Financial Intelligence Unit under clause (c) of sub-section 23(1) of MLPA, 2012, Bangladesh Financial Intelligence Unit may impose a fine on such organization 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.

(e) If any person or entity or reporting organization fails to pay any fine imposed by Bangladesh Financial Intelligence Unit under sections 23 and 25 of this Act, Bangladesh Financial Intelligence Unit 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 Financial Intelligence Unit, and in this regard if any amount of the fine remains unrealized, Bangladesh Financial Intelligence Unit may, if necessary, make an application before the court for recovery and the court may pass such order as it deems fit.

(f) If any reporting organization is imposed fine under sub-sections 23 (3), (4), (5) and (6), Bangladesh Financial Intelligence Unit 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 Employee or persons employed on contractual basis of that reporting organization and, where necessary, may direct the relevant organization to take necessary administrative actions.

Penalties for non-compliance of Anti-Terrorism (Amendment) Act, 2013

(a) If any reporting agency fails to comply with the directions issued by Bangladesh Financial Intelligence Unit 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 Financial Intelligence Unit not exceeding Taka 10 (ten) lacs and Bangladesh Financial Intelligence Unit may suspend the registration or license with intent to stop operation of the said agency or any of its branches 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. [U/S 16(3) of ATA 2012]

(b) If any reporting agency fails to pay or does not pay any fine imposed by Bangladesh Financial Intelligence Unit according to sub-section 16 (3) of ATA, Bangladesh Financial Intelligence Unit may recover the amount from the reporting agency by debiting its accounts maintained in any bank or financial institution or Bangladesh Bank and in case of any unrealized or unpaid amount, Bangladesh Financial Intelligence Unit may, if necessary, apply before the concerned court for recovery. [U/S 16(4) of ATA 2012]

"Safe Harbor" Provision for Reporting

Safe harbor laws encourage financial institutions to report all suspicious transactions by protecting financial 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.

Appendix 1: Database of OFAC to be checked

Relationship Manager must be checked the following database before making any relationship with client(s) and distribute the list time to time by CAMLCO:

i. Checking the Office of Foreign Assets Control (OFAC) Lists

Before engaging in any money service activity (including but not limited to check cashing, money orders and wire transfers) which potentially may involve money laundering, and on an ongoing basis, we will check to ensure that a customer does not appear on the OFAC "Specifically Designated Nationals and Blocked Persons" List, SDN List, and is not from, or engaging in transactions with people or entities from, embargoed countries and regions listed on the OFAC website Because the OFAC Website is updated frequently, we will consult the list on a regular basis and subscribe to receive updates when they occur. We may, if necessary, access these lists through various software programs to ensure speed and accuracy. We will also review existing accounts against these lists when they are updated and we will document our review.

ii. Comparison with Bangladesh Financial Intelligence Unit provided lists of terrorists and other criminals

MFIL may receive, from time to time, list of known or suspected terrorists form Bangladesh Financial Intelligence Unit. Within a reasonable period of time after an account is opened or transaction is completed (or earlier, if required by another laws and regulation or directive issued in connection with an applicable list), we will determine whether a customer appears on any such list of known or suspected terrorists or terrorist organizations issued by any government agency.

Appendix 2: Enhance Due Diligence (EDD) for PEPs, Influential Persons and High Level Management in International Organizations

While opening and/or operating account of Politically Exposed Persons (PEPs) enhanced due diligence shall have to be exercised. Following instructions shall have to be followed to ensure Enhanced Due Diligence (EDD):

- take reasonable measures to establish the source of wealth and source of funds;
- ongoing monitoring of the transactions have to be conducted; and
- The Account Opening Officer should observe all formalities as detailed in Guidelines for Foreign Exchange Transactions while opening accounts of non-residents.

In keeping with the assessment of risk and the allowance for simplified CDD where risk is low, there is a requirement to have EDD where risk is high e.g. relationship with PEPs.

The instructions in relation to Politically Exposed Persons as contained in ML circular no. 14 dated 25 September 2007 stand substituted as follows:

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

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"*.

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

Following instructions shall have to be followed to ensure Enhanced Due Diligence, while opening and operating the account of Politically Exposed Persons (PEPs):

(a) a risk management system shall have to be introduced to identify risks associated with the opening and operating accounts of PEPs;
(b) obtain senior management approval for establishing business relationships with such customers;
(c) take reasonable measures to establish the source of wealth and source of funds;
(d) ongoing monitoring of the transactions have to be conducted; and
(e) MFIL should observe all formalities as detailed in Guidelines for Foreign Exchange Transactions while opening accounts of non-residents, if any.

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

Apart from that, while establishing and maintaining business relationship and conducting 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 enlisted in Financial Action Task Force's Non-cooperating Countries and Territories list) enhanced due diligence shall have to be ensured.

Responsibilities in case of "Influential Persons":

Bank/FI has to identify the true underlying beneficiaries against the account and/or client. If establishing and maintaining banking relationship with such personnel is deem risky, Bank/FI has to follow the instructions as cited as above from point "b" to "d"

By "Influential Person" it is meant-" individuals who are or have been entrusted domestically with prominent public functions, for example Head of State or of Government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials."

Instructions appropriate for Influential persons shall also be applicable for close associates.

No middle ranking or more junior individuals shall be deemed as "Influential Person" as quoted in this paragraph.

Responsibilities in case of Head of any International Organization or High Level Officers:

Bank/FI has to identify whether the account and/or client is truly benefiting the head of any international organization or any high level officers.

If establishing and maintaining banking relationship with such personnel is deem risky, Bank/FI has to follow the instructions as cited as above from point "b" to "d" and instructions as suggested in "e" should also be followed in appropriate cases. Instructions appropriate for head of any international organization or any high level officers shall also be applicable for his/her close associates.

By "Head of International Organization or High Level Officers" it is meant- persons who are or have been entrusted with a prominent function by an international organization refers to members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions"

Instructions as appropriate for "Head of International Organization or High Level Officers" are also applicable for their close associates.

No middle ranking or more junior individuals shall be deemed as "Head of International Organization or High Level Officers" as quoted in this paragraph.

Ongoing monitoring of accounts and transactions

On-going monitoring is an essential aspect of effective CDD procedures. Effectively internal control system may reduce the risk if relationship managers have an understanding of normal and reasonable account activity of their customers so that they have a means of identifying transactions which fall outside the regular pattern of an account's activity. Without such knowledge, they are likely to fail in their duty to report suspicious transactions to the appropriate authorities in cases where they are required to do so. The extent of the monitoring needs to be risk-sensitive. For all accounts, we have to ensure proper systems in place to detect unusual or suspicious patterns of activity. Particular attention should be paid to transactions that exceed these limits. Certain types of transactions should alert management to the possibility that the customer is conducting unusual or suspicious activities. They may include transactions that do not appear to make economic or commercial sense, or that involve large amounts of cash deposits that are not consistent with the normal and expected transactions of the customer. Very high account turnover, inconsistent with the size of the balance, may indicate that funds are being "washed" through the account.

There should be intensified monitoring for higher risk accounts. MFIL should set key indicators for such accounts, taking note of the background of the customer, such as the country of origin and source of funds, the type of transactions involved, and other risk factors.

To ensure that records remain up-to-date and relevant, there is a need for MFIL 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 MFIL 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.

MFIL has developed clear standards on what records must be kept on for customer identification and individual transactions and their retention period. As the starting point and natural follow-up of the identification process, MFIL should obtain customer identification papers and retain copies of them for at least five years after an account is closed. They should also retain all financial transaction records for at least five years after the transaction has taken place.

Appendix 3: DECLARATION OF MANAGING DIRECTOR ON AML/CFT

Introduction of MFIL

Meridian Finance & Investment Limited (MFIL) take the opportunity to introduce ourselves as a fast growing Multi-product Non-bank Financial Institution licensed by Bangladesh Bank, with a paid-up capital of BDT 1,200 million and a shareholding structure consisting of 79% Institutional and 21% individual stakeholders.

The Board of the MFIL is composed of very successful people in their field of work and profession with high level of business acumen and leadership qualities. MFIL Chairman Mr. Kazi Aminul Islam was an Alternative Executive Director of The World Bank and a Secretary, Prime Minister's Office. MFIL sponsors include renowned business conglomerates with strong equity base such as RSRM, Habib Group, Toma Group, Labib Group, Elegant Group, Saad Musa Group, Ahsan Group, Rising Group, and Gold Star Group.

MFIL was incorporated in Bangladesh on January 15, 2014 as public limited company. The Company was licensed under Financial Institutions Act, 1993 by Bangladesh Bank on June 04, 2015 and started operation from December 2015. The registered office of the Company is situated at Silver Tower (Level-6), 52 Gulshan Avenue, Gulshan - 1 Dhaka – 1212, Bangladesh.

The Regulator

Bangladesh Bank, the Central Bank of Bangladesh, is the regulatory and supervisory authority for banks and financial institutions in the Country. Bangladesh Financial Intelligence Unit issued a number of regulations for combating Money Laundering (ML) and Terrorist Financing (TF) activities in Bangladesh. Guided by these rules and regulations MFIL has reviewed, updated, developed and implemented AML/CFT policies and procedures including the Know Your Customer Policy. The policies and procedures are under constant review for improvement under guidelines issued by Bangladesh Financial Intelligence Unit.

Outline of ML/TF

Money laundering is the process of concealing sources of money. Money which is evidently the proceeds of a crime is referred as "dirty money", and money which has been "laundered" to appear legitimate is referred to as "clean money". Fundamental concept of money laundering is the process by which proceeds from a criminal activity are attempted to be concealed of their illicit origins. The conversion or transfer of property, knowing that such property is derived from any offense, e.g. drug trafficking, or offenses or from

an act of participation in such offense or offenses, for the purpose of concealing the illicit origin of the property or of assisting any person who is involved in the commission of such an offense or offenses to evade the legal consequences of his actions.

Terrorist financing means funds financed for terrorist activity. It may involve funds raised from legitimate sources, such as personal donations and profits from businesses and charitable organizations, as well as from criminal sources, such as the drug trade, the smuggling of weapons and other goods, fraud, kidnapping and extortion. Terrorists use techniques like those of money launderers to evade authorities' attention and to protect the identity of their sponsors and of the ultimate beneficiaries of the funds. However, when terrorists raise funds from legitimate sources, the detection and tracking of these funds becomes more difficult.

Why against ML/TF

As criminals require financial services in order to launder the proceeds of and fund their criminal activities, money laundering and terrorism not only harm the public but can also damage the stability and reputation of the financial sectors as a whole. It is obvious that the financial institutions shall take reasonable measures to prevent ML/TF for its own self as well as the society at large. Thus, appropriate procedures must be in place within financial institutions to assist Bangladesh Financial Intelligence Unit as well as Government and related foreign bodies in their effort for combating ML/TF.

MFIL's Declaration

It is of great importance, like other financial institutions, that MFIL acts for combating the risk of money laundering and terrorist financing in collaboration with Bangladesh Financial Intelligence Unit as well as the Government and related foreign bodies. Therefore, MFIL hereby declares and confirms that:

1. it is an institution licensed under Financial Institution Act, 1993 by Bangladesh Bank and duly supervised and regulated by Bangladesh Bank and other supervisory authorities of Bangladesh;

2. it is subject to and compliant with all applicable laws and regulations relating to the ML/TF issues including client due diligence obligations and obligations relating to the cooperation with public authorities, and has implemented written procedures and internal control mechanism in order to comply with Money Laundering Prevention Act, 2012 and Anti-Terrorism Act, 2009 (both Acts are as amended up to 2013) and its regulations;

3. it has adopted a Board approved policy on prevention ML/TF and implemented effective program to comply with applicable laws and regulations;

4. it applies self-assessment and independent testing procedures towards gap analysis for ensuring that our business units are compliant with applicable ML/TF laws and regulations;

5. it applies procedures regarding Know Your Customer and Customer Due Diligence to identify the customer and verification of customer's identity on the basis of documents, data or information provided by them, and where applicable we take the same procedures on the beneficial owner;

6. it relies on those who are close to our customers such as relationship officer, branch manager, customer service officer to understand fully with whom we are doing business and to ensure that the business we conduct on behalf of our customers is legitimate;

7. it applies procedures/judgment to identify suspicious transaction and activity to mitigate/minimize as defined in the Money Laundering Prevention Act (MLPA)-2012 and Anti-Terrorism Act-2009. MFIL, its Directors, officers and employees restrict themselves to disclose the fact that an STR/SAR or any related information are being reported to BFIU;

8. it keeps correct and full records of the customers at least for five years after closing of relationship as per section 25(1) of Money Laundering Prevention Act-2012;

9. it administers/combats ML/TF issues by engaging CAMLCO, DCAMLCO, and with a strong Central Compliance Unit and other Committees as per instruction of Bangladesh Financial Intelligence Unit;

10. it applies ongoing monitoring measures, including regular screenings of the sanctions lists issued by The United Nations Security Council Resolution 1267 & 1373 and ensures that its customer files are checked regularly before any financial transaction;

11. it does and will not hold assets on behalf of customers or beneficial owner of the customers a) domiciled in jurisdiction which, according to the listings published by the FATF, is a high risk and non-cooperative jurisdiction or b) which are subject to UN sanctions; and

12. We are fully committed to remaining constantly alert to prevent the use of our products and services by those who are likely to abuse them.

We promise that:

1. we will develop and continue to update ML/TF guidelines periodically to meet applicable legal and regulatory requirements, if any, circulated by Bangladesh Financial Intelligence Unit and other regulatory authorities;

2. we will assist Bangladesh Financial Intelligence Unit and other regulatory authorities to identify relevant information with regard to identifying customer/entities who are related to the ML/TF activities;

3. we will take necessary procedures to monitor transactions for the purpose of identifying possible suspicious transactions or activities;

4. we will take initiative to train employees through internal and external training programs and assist them for building capacity to combat ML/TF;

5. we will not allow direct use of correspondent accounts by third parties to transact business on customer's behalf;

6. we will introduce Know Your Employee program and procedures to understand employees background, conflicts of interest and susceptibility to ML/TF complicity; and

7. we will not allow/maintain any anonymous account.

Appendix 4: Uniform Account Opening Form

Appendix 5: Internal Control Checklist

Sl. No.	Particular of Control	Yes/No
1	Have you carried out a review of processes in your business to identify where money laundering is most likely to occur?	
2	Is this review regularly updated?	
3	Have you established procedures and controls to prevent or detect money laundering?	
4	Is the effectiveness of such controls tested?	
5	Do online or electronic transactions circumvent these controls?	
6	Do you have a comprehensive written policy on money laundering?	
7	Is all Employee aware of this policy?	
8	Does your money laundering policy include clear guidelines on accepting corporate hospitality and gifts?	
9	Is all Employee aware of their responsibilities with regard to money laundering?	
10	Do they receive regular money laundering training?	
11	Are all members of Employee sufficiently capable of identifying suspicious transactions?	
12	Are your systems capable of highlighting suspicious transactions (i.e. those not conforming to usual parameters)?	
13	Do all members of Employee know the identity of their Chief Anti Money Laundering Compliance Officer (CAMLCO)?	
14	Are your systems capable of providing the CAMLCO will all the information required for the Annual Management Report?	
15	Do you thoroughly check and verify the identity of all your clients?	
16	Do you have client accounts in the name of fictitious persons/ entities?	
17	Do you know the identity of the beneficial owner of all your corporate clients?	
18	Is this identity verified?	
19	Are all suspicious transactions reported to BFIU?	

Signature: _____

Name : _____

Date:_____ Designation: Head of Internal Audit & Compliance

Appendix 6: Internal Suspicious Activity Report Form

A. Reporting Institution :

1. Name of the FI:
2. Name of the Branch:

B. Details of Report:

1. Date of sending report:
2. Is this the addition of an earlier report? Yes ☐ No ☐
3. If yes, mention the date of previous report

C. Suspect Account Details :

1. Account Number:
2. Name of the account:
3. Nature of the account:
(FDR/loan/other, pls. specify)
4. Nature of ownership:
(Individual/proprietorship/partnership/company/other, pls. specify)
5. Date of opening:
6. Address:

D. Account holder details :

1. 1. Name of the account holder:
   2. Address:
   3. Profession:
   4. Nationality:
   5. Other account(s) number (if any):
   6. Other business:
   7. Father's name:
   8. Mother's Name:
   9. Date of birth:
   10. TIN/E-TIN:
2. 1. Name of the account holder:
   2. Relation with the account holder mention in sl. no. D1
   3. Address:
   4. Profession:
   5. Nationality:
   6. Other account(s) number(if any):

7. Other business:	
8. Father's name:	
9. Mother's Name:	
10. Date of birth:	
11. TIN/E-TIN:	

E. Introducer Details :

1. Name of introducer:	
2. Account number:	
3.Relation with account holder:	
4. Address:	
5. Date of opening:	
6. Whether introducer is maintaining good relation with FI:	

F. Reasons for considering the transaction(s) as unusual/suspicious?

a. ☐ Identity of clients
b. ☐ Activity in account
c. ☐ Background of client
d. ☐ Multiple accounts
e. ☐ Nature of transaction
f. ☐ Value of transaction
g. ☐ Other reason (Pls. Specify)

_____

_____

(Mention summery of suspicion and consequence of events)
[To be filled by the BAMLCIO]

G. Suspicious Activity Information

Summary characterization of suspicious activity:

a.	☐ Bribery/Gratuity	h.	☐ Counterfeit debit/credit card	o.	☐ Mortgage Loan Fraud
b.	☐ Check Fraud	i.	☐ Counterfeit instrument	p.	☐ Mysterious Disappearance
c.	☐ Check Kitting	j.	☐ Credit card fraud	q.	☐ Misuse of Position or Self-Dealing
d.	☐ Commercial loan fraud	k.	☐ Debit card fraud	r.	☐ Structuring
e.	☐ Computer intrusion	l.	☐ Defalcation/Embezzlement	s.	☐ Terrorist Financing
f.	☐ Consumer loan fraud	m.	☐ False statement	t.	☐ Wire Transfer Fraud
g.	☐ Counterfeit check	n.	☐ Identity Theft	u.	Other _____

H. Transaction Details:

Sl. no.	Date	Amount	Type*

**Cash/Transfer/Clearing/DD/PO/etc.*
Add paper if necessary

I. Counter Part's Details					
Sl. no.	Date	Bank	Branch	Account no.	Amount

J. Has the suspicious transaction/activity had a material impact on or otherwise affected the financial soundness of the FI? Yes ☐ No ☐

K. Has the FI taken any action in this context? If yes, give details.

L. Documents to be enclosed
1. Account opening form along with submitted documents 2. KYC Profile 3. Account statement for last one year 4. Supporting voucher/correspondence mention in sl. no. H 5. Others

Appendix 7: Know Your Employee*

(This is a sample version of KYE Form. Any other version of KYE will also be accepted provided that the purpose will be fulfilled)

1. Personal Details:

FULL NAME (ENGLISH)	MR./ MS.		
EMPLOYEE ID		INSURANCE ID	
DESIGNATION		DEPARTMENT	
DATE OF BIRTH		PLACE OF BIRTH	
PERMANENT ADDRESS		PRESENT ADDRESS	
DATE OF JOINING		CONFIRMATION DATE	
TYPE OF EMPLOYMENT	□ PERMANENT	□ CONTRACTUAL	□ Other
REFERENCE			
BLOOD GROUP		RELIGION	

2. Family Details:

MOTHER'S NAME	
MOTHER'S PROFESSION	
FATHER'S NAME	
FATHER'S PROFESSION	
SPOUSE NAME	
SPOUSE PROFESSION	

3. Educational Background:

EDUCATIONAL QUALIFICATION	INSTITUTIONS NAME	RESULTS
S.S.C		
H.S.C		
BACHELORS'		
MASTERS'		
PROFESSIONAL DEGREE		

4. Professional Background:

EMPLOYER'S NAME	ADDRESS	DESIGNATION	DEPARTMENT	CONTACT NUMBER	FAX NUMBER	RELEASE ORDER RECEIVED FROM PREVIOUS EMPLOYER

5. Identification:

NATIONAL ID	
PASSPORT NUMBER (IF ANY)	
TIN NUMBER (IF ANY)	
DRIVING LICENSE (IF ANY)	

6. Contact Details

PRESENT ADDRESS		
PERMANENT ADDRESS		
PHONE NUMBER (MOBILE)		
PHONE NUMBER (RESIDENT)		
PHONE NUMBER (OFFICE)		
EMAIL ADDRESS (PERSONAL)		
EMAIL ADDRESS (OFFICE)		
EMERGENCY CONTACT NAME & PHONE NO.		
RELATIONSHIP WITH EMPLOYEE		

7. Others

POLITICAL INVOLVEMENT	□ YES □ NO	RESIDING AT	□ RENTED HOUSE □ OWN
IF RENTED FROM HOW MANY RESIDENCE YOU HAVE CHANGED IN LAST 5 YEAR:			
DOING PART TIME JOB WITH OTHER ORGANIZATION		□ YES	□ NO
IF YES, PLEASE PROVIDE THE NAME OF THE ORGANIZATION AND POSITION			
INVOLVEMENT WITH ANY OTHER BUSINESS		□ YES	□ NO
IF YES, PLEASE PROVIDE THE NAME OF THE BUSINESS			
IMMEDIATE PREVIOUS RESIDENCE ADDRESS			
TRAVEL RECORD (ABROAD)		OWNED VEHICLE	□ YES □ NO

Declaration: I hereby declare and confirm that all the information as given above are true and correct.

_____

Signature of the Employee with date

To be filled up by Human Resource Department

ATTESTED COPY OF EDUCATIONAL CERTIFICATES RECEIVED	□ YES □ NO
ORIGINAL COPY OF EDUCATIONAL CERTIFICATES SEEN	□ YES □ NO
POLICE CLEARANCE CERTIFICATE	□ YES □ NO
KYE REVIEW DATE	

List of Abbreviations

ML	Anti Money Laundering
CAMLCO	Chief Anti Money Laundering Compliance Officer
BAMLCO	Branch Anti-Money Laundering Compliance Officer
BFIU	Bangladesh Financial Intelligence Unit
CDD	Customer Due Diligence
CCU	Central Compliance Unit
CEO	Chief Executive Officer
CTR	Cash Transaction Report
CPV	Contact Point Verification
CTF	Combating Terrorist Financing
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
KYC	Know Your Client
MFIL	Meridian Finance & Investment Limited
MLPA	Money Laundering Prevention Act
MD	Managing Director
OFAC	Office of Foreign Assets Control
PEP	Politically Exposed Person
SOP	Standard Operating Procedure
SDN	Specifically Designated Nationals and Blocked Persons
STR	Suspicious Transaction Report
SAR	Suspicious Activity Report
TP	Transaction Profile
BB	Bangladesh Bank
BoD	Board of Directors
BAC	Board Audit Committee