# FAREAST FINANCE & INVESTMENT LIMITED

A Financial Institution licensed by Bangladesh Bank
under The Financial Institutions Act, 1993

# Prevention of Money Laundering and Terrorist Financing Manual

**April 2018**

Eunoos Center (8th level)
52-53 Dilkusha Commercial Area, Dhaka-1000, Bangladesh
Phone: 880-2-7162328, 9554174, 9559621, 9563253, 9572169, 01819245908
E-mail: ffil@bdcom.net, Web site: http://www.ffilbd.com

**Fareast Finance & Investment Limited**
**Prevention of Money Laundering and Terrorist Financing Manual**

## Contents

**Fareast Finance & Investment Limited**
**Prevention of Money Laundering and Terrorist Financing Manual**

## Section-1: Introduction

### 1.1 Short title

This manual may be called the Prevention of Money Laundering and Terrorist Financing Manual of Fareast Finance & Investment Limited.

### 1.2 Background

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 United Nations (UN) was the first international organization to undertake significant actions to fight against money laundering through adopting several conventions and resolutions. Following UN action, the Financial Action Task Force on Money Laundering (FATF) was formed by G-7 countries in 1989 as the first intergovernmental body which has recommended 40 recommendations to combat money laundering in 1990. In October 2001, the FATF expanded its mandate to deal with the funding of terrorist acts and terrorist organization, and it took the important step of creating the 8 (later expanded to 9) Special Recommendations on Terrorist Financing. These 40+9 recommendations have been endorsed by over 180 countries and are universally recognized as international standard for Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT) program.

To oversee the implementation of these recommendations in Asia Pacific Region, the Asia/Pacific Group on Money Laundering (APG), FATF-style regional body, was founded in 1997, of which Bangladesh is a founding member. FATF has further extended its mandate to include Proliferation Financing and accumulated all 40+9 recommendations into 40 Recommendations in February 2012.

In line with the international initiatives and standards, Bangladesh has also enacted Money Laundering Prevention Act (MLPA), 2012 (Ammended 2015), (repealing the MLPA, 2009) and Anti Terrorism Act (ATA), 2009 (as amended in 2012). The new acts address all the deficiencies identified in the 2nd Mutual Evaluation of Bangladesh

conducted by APG in 2008 to determine the extent of its compliance, with the global standards. Both the Acts have empowered Bangladesh Financial Intelligence Unit (BFIU) to perform the anchor role in combating ML and TF through issuing guidance and directives for reporting agencies including Financial Institutions (FIs), as defined in section 2(g) of MLPA, 2012 (Amended 2015).

This manual is in conformity with international standard and laws and regulations enforceable in Bangladesh. Board Audit Committee of FFIL shall review and confirm the meticulous compliance of this manual and the circulars issued by Bangladesh Financial Intelligence Unit (BFIU) in this regard to be reported by the FFIL's Compliance Department directly on quarterly basis.

## 1.3 Scope

### 1.3.1 Objectives

The standards set out in this manual are the minimum requirements based on applicable legal and regulatory requirements in compliance with the Anti-Money laundering Act, 2012,( Amended 2015) Anti Terrorism Act (ATA), 2009 (as amended in 2012) and Bangladesh Financial Intelligence Unit (BFIU)guidelines, circulars in this respect. These requirements are intended to prevent FFIL, its Executives and clients from being misused for money laundering, terrorist financing or other financial crime(s).

### 1.3.2 Applicability

According to section 25 of the Anti-Money laundering Act, 2012,( Amended 2015) FFIL Board of Directors through the company Executives must ensure that the legal duties resulting from the regulations set out in this Act and Bangladesh Financial Intelligence Unit (BFIU) guidelines regarding AML are fulfilled by all of FFIL's subordinated enterprises, branches, subsidiaries and affiliates in Bangladesh and abroad. Wherever any regulations are stricter than the requirements set out in this manual, the stricter standard has to be applied. If any applicable laws are in conflict with this manual, the relevant entity must consult with the legal department and the Chief Anti Money Laundering Compliance Officer to resolve the conflict.

If the minimum requirements set out in this manual cannot be applied in a certain country for the subordinated enterprises, branches, subsidiaries and affiliates, because of local law or cannot be enforced due to other than legal reasons, it is to be ensured that FFIL will not

- enter into a business relationship,
- continue a business relationship or
- carry out any transactions.

If business relations already exist in that country, it has to be ensured that the business relationship is terminated regardless of FFIL's other contractual or legal obligations.

## 1.4 Definition of Money Laundering

Money Laundering is the participation in any transaction that seeks to conceal or disguise the nature or origin of funds derived from illegal activities, e.g., fraud, corruption, organized crime, or terrorism etc. According to Section 2(v) of the Money Laundering Prevention Act 2012 (Amended 2015) "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;

## 1.5 Reasons of Money Laundering

First, money represents the lifeblood of the organization/person that engages in criminal conduct for financial gain because it covers operating expenses and pays for an extravagant lifestyle. To spend money in these ways, criminals must make the money they derived illegally appear legitimate.

Second, a trail of money from an offense to criminals can become incriminating evidence. Criminals must obscure or hide the source of their wealth or alternatively disguise ownership or control to ensure that illicit proceeds are not used to prosecute them.

Third, the proceeds from crime often become the target of investigation and seizure. To shield ill-gotten gains from suspicion and protect them from seizure, criminals must conceal their existence or, alternatively, make them look legitimate.

## 1.6 Stages of Money Laundering

There is no single method of laundering money. Methods can range from the purchase and resale of a luxury item (e.g. a house, car or jewelry) to passing money through a complex international web of legitimate businesses and 'shell' companies (i.e. those companies that primarily exist only as named legal entities without any trading or business activities). There are a number of crimes where the initial proceeds usually take the form of cash that needs to enter the financial system by some means. Bribery, extortion, robbery and street level purchases of drugs are almost always made with cash. These proceeds of crime have to enter the financial system by some means so that it can be converted into a form which can be more easily transformed, concealed or transported. The methods of achieving this are limited only by the ingenuity of the launderer and these methods have become increasingly sophisticated. Despite the variety of methods employed, money laundering is not a single act but a process accomplished in three basic stages which are as follows:

**Placement:** The introduction of illegally obtained monies or other valuables into financial or non-financial institutions.

**Layering:** Separating the proceeds of criminal activity from their source through the use of layers of complex financial transactions. These layers are designed to hamper the audit trail, disguise the origin of funds and provide anonymity.

**Integration:** Placing the laundered proceeds back into the economy in such a way that they re-enter the financial system as apparently legitimate funds.

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

## 1.7 Definition of Terrorist Financing

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

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

    a) An act which constitutes an offence within the scope of and as defined in one of the treaties listed in the link given below; or
    b) Any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking any active part in the hostilities in

a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing an act.

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

According to the article 7 of the Anti Terrorism (Amendment) Act, 2012 of Bangladesh, financing of terrorism means: Offences relating to financing terrorist activities if:

(i) 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.

(ii) 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.

(iii) 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.

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

### 1.8 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.

**1.9 Interpretation**

In this manual, unless there is anything repugnant in the law, subject or context:

1.9.1 "Company" means Fareast Finance & Investment Limited (FFIL).
1.9.2 "The Board" means the Board of Directors of the company.
1.9.3 "The Management" means the persons who are in the policy implementation and operational aspect of the company.
1.9.4 "Managing Director" means the Chief Executive of the company.
1.9.5 "Executive" means an Executive of the company whether temporary or permanent classified as such and includes an Executive on probation.
1.9.6 "AML/CFT AMLD" means Anti-Money Laundering/Combating the Financing of Terrorism Anti-Money Laundering Department.
1.9.7 "APG" means Asia Pacific Group on Money Laundering.
1.9.8 "ATA" means Anti Terrorism Act.
1.9.9 "BAMLCO" means Branch Anti-Money Laundering Compliance Officer.
1.9.10 "BFIU" means Bangladesh Financial Intelligence Unit .
1.9.11 "BDT" means Bangladesh Taka.
1.9.12 "BFIU CAMLCO" means Bangladesh Financial Intelligence Unit Chief Anti-Money Laundering Compliance Officer.
1.9.13 "CCU" means Central Compliance Unit.
1.9.14 "CDD" means Customer Due Diligence.
1.9.15 "CTC" means Counter Terrorism Committee.
1.9.16 "CTR" means Cash Transaction Report.
1.9.17 "FATF" means Financial Actions Task Force.
1.9.18 "FI FIU FSRB" means Financial Institution Financial Intelligence Unit ATF Style Regional Body.
1.9.19 "GPML" means Global program against Money Laundering.
1.9.20 "ICRG" means International Cooperation and Review Group.
1.9.21 "IOSCO" means International Organization of Securities Commissions.
1.9.22 "KYC" means Know Your Customer.
1.9.23 "ML" means Money Laundering.
1.9.24 "MLPA" means Money Laundering Prevention Act.
1.9.25 "NCC" means National Coordination Committee.
1.9.26 "NCCT" means Non-cooperating Countries and Territories.
1.9.27 "OECD" means Organization for Economic Co-operation and Development.
1.9.28 "PER" means Politically Exposed Persons.
1.9.29 "STR" means Suspicious Transaction Report.
1.9.30 Words importing persons include both male and female employees of the company.
1.9.31 Words importing singular number shall include the plural and vice versa.

### 1.10 Variation, modification and amendment of manual

The Board of Directors of the company if required in the interest of the company and to comply with Bangladesh Financial Intelligence Unit (BFIU) guidelines/circular/circular letter, may vary, modify, incorporate, amend or cancel any of the rules and regulations regarding this manual. Besides, the Board of Directors of the company if required in the interest of the company and to comply with Bangladesh Financial Intelligence Unit (BFIU)guidelines/circular/circular letter, may reform the CCU at any time. Besides, Board of Directors of FFIL shall review this manual on yearly basis if required.

## Section-2: Vulnerabilities of Products and Services and their overcome procedure

### 2.1 Lease/Term loan finance

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

### 2.2 Factoring

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

### 2.3 Private placement of equity/securitization of assets

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

### 2.4 Personal loan/car loan/home loan

Any person can take personal loan from FIs and repay it by illegally earned money; thus he/she can launder money and bring it in the formal channel. After taking home loan or car loan, money launderers can repay those with their illegally earned

money, and later by selling that home/car, they can show the proceeds as legal money.

**2.5 SME/Women entrepreneur loan**

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

**2.6 Deposit scheme**

FIs can sell deposit products with at least a six months maturity period. However, the depositor can encash their deposit money prior to the maturity date with prior approval from Bangladesh Financial Intelligence Unit (BFIU), 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.

**2.7 Loan backed money laundering**

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

**2.8 Vulnerabilities overcome procedure**

To overcome the above vulnerabilities FFIL shall take the following measures in future:

- Develop sufficient capacity to verify the identification and source of funds of their clients.
- Human resources will be trained to become skilled enough for tracing money laundering and terrorist financing activities.
- To introduce anti-money laundering software for monitoring and report regarding transactions of a suspicious nature to the financial intelligence unit of BB.

.

## Section-3: Compliance requirement

FFIL in all cases shall comply with the provisions of Money Laundering Prevention Act, 2012 (Amended 2015), Anti terrorism (Amendment) Act, 2012 and circulars/ instructions issued by BFIU of BB in these regards. To implement this manual and compliance of instructions of BB, FFIL shall designate one high level Executive as Chief Anti-Money Laundering Compliance Officer (CAMLCO) in the Central Compliance Unit (CCU) and one officer as Branch Anti-Money Laundering Compliance Officer (BAMALCO) in the branch level. Besides, for day-to-day works FFIL Head Office, subordinated enterprises, branches, subsidiaries and affiliates shall comply with the following basic principles:

### 3.1 Customer identification

3.1.1 For prevention of money laundering and terrorist financing it is mandatory to collect and verify the correct and complete identification of customers. For this purpose, FFIL shall define its customers as follows:

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

3.1.2 FFIL shall identify its customers in the following cases:

- While entering into a lasting business relationship;
- While performing a single transaction or deal;
- While conducting financial transaction with the existing customer;
- Before accepting cash or other physical values worth equivalent or more of BDT 500,000 outside an existing business relationship.

3.1.3 Whenever it is required to identify a customer, FFIL shall establish and verify the identity of the ultimate natural person,

- who owns or
- controls the customer or its assets or
- on whose behalf the transaction is carried out or the business relationship is established

### 3.2 Establishment of purpose of business relationship

When entering into a lasting business relationship, FFIL shall obtain information on kind and purpose thereof, if this is not clear from the business relationship itself. Customer due diligence shall be performed for high risk customers, non face to face business (if applicable), handling of PEPs. In this case "PEPs" shall be those 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. For opening account in favor PEPs, FFIL should follow the instructions of Foreign Exchange Regulation Act, 1947

**3.3 Identification of ultimate beneficial owner**

On the basis of the information obtained from reliable sources, FFIL shall identity the beneficial owner of the business/account and perform the followings:

- If a customer operate an account on behalf of another person in his/her own name, FFIL shall collect and preserve the complete and correct information of identity of the person(s) besides the customer.
- FFIL shall identify the controller or the owner of the customer.
- FFIL shall collect and preserve the complete and correct information of identity of the beneficial owner(s) of the customer. For this purpose, a person will be treated as a beneficial owner if:
  (a) he has controlling share of a company and/or
  (b) hold 20% or more shares of a company.

**3.4 Client account monitoring**

FFIL shall monitor its customers' account(s) including their business pattern/behavior through inspection/record verification on annual basis to detect unusual/suspicious transactions. In case any unusual/suspicious transactions are found, FFIL shall take appropriate measures for STR to BB.

**3.5 Reporting of suspicious circumstances/transactions (STR)**

3.5.1 According to Section 2(z) of MLPA 2012 suspicious transaction shall mean such transaction:

- which deviates from usual transactions;
- of which there is ground to suspect that,
  - the property is the proceeds of an offence
  - it is financing to any terrorist activity, a terrorist group or an individual terrorist;
- any other transaction or attempt of transaction delineated in the instructions issued by Bangladesh Financial Intelligence Unit (BFIU)from time to time.

3.5.2 In the above circumstances/transactions FFIL shall report to Bangladesh Financial Intelligence Unit (BFIU) through STR. CAMLCO and BCAMLCO shall always be informed about all suspicious circumstances/transactions.

**3.6 Correspondent business**

FFIL shall pay special attention to business done only through correspondent.

**3.7 Staff reliability**

It is the responsibility of each employee to become familiar with rules and regulations that relate to his or her assignment. Moreover, disciplinary action would be taken if employees consistently fail to perform in accordance with AML/CFT framework for

a consecutive period of six months. Besides, FFIL shall complete the KYE before appointment in the company.

**3.8 Communicating the policies**

The Managing Director shall communicate to all employees on annual basis through a statement that clearly sets the policy against money laundering and any activity which facilitates money laundering or the funding of terrorist or criminal activities. This statement shall also be submitted to the Board of Directors via Board Audit Committee. This statement shall include the following:

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

**3.9 Anti Money Laundering controls**

FFIL shall ensure that all applicable AML requirements are being adhered to and security measures are properly functioning in the company in all respects.

**3.10 Employee appointment and training**

Before appointing any employee FFIL shall perform the screening mechanism through KYE in details with proper records/documents. Within two months of appointment all employees (including trainees and temporary personnel) responsible for carrying out transactions and/or for initiating and/or establishing business relationships shall undergo anti money laundering training process and subsequently after every three years. Chief Anti Money Laundering Compliance Officer shall fix the training modules. Besides, if management thinks proper, FFIL may time to time distribute leaflets among customers to make them aware about money laundering and terrorist financing and also arrange to stick posters in every branch at a visible place.

FFIL shall perform the screening mechanism through the following ways:

1) NID verification through the website of Election Commission;
2) CMMS verification through Corporate Memory Management System of Bangladesh Bank;

3) Verification through UN sanction lists and local sanction lists screening.
4) Verification of the highest obtained certificate.

If at any time subsequent to the appointment, any employee of the company is accused and proved of ML/TF or his/her negligence on the said issue, the company will duly inform Bangladesh Bank and take necessary action against the employee in relation with the existing law of the country and Bangladesh Bank guidelines and circulars.

**3.11 Anti Money Laundering risk analysis**

At the time of analyzing the credit risk, FFIL Executives shall analyze the Anti Money Laundering risk exposure considering product and client risk and mitigate the same.

**3.12 UN sanctions**

FFIL shall take all necessary actions on UNSCR 1267 and 1373 (targeted financial sanctions). To comply with this direction, FFIL shall prepare a software regarding the UN sanction list for regular searching and if find any account with it, shall inform BFIU immediately.

## Section-4: Risk Assessment Procedure of FFIL

The success of AML&CFT program highly depends on efficient assessment of related threat/vulnerability/risk and placing necessary tools for combating ML&TF risks as per the result of assessed threat/vulnerability/risk. FFIL is trying to categorize the risks which will help determine the level of AML&CFT resources necessary to mitigate that risk assessment process is developed to take appropriate steps to identify and assess the company's money laundering and terrorist financing risks for customers, countries or geographic areas, products, services and transactions or delivery channels.

### 4.1 Risk group: Customers

| Risk | Likelihood | Impact | Risk score | Treatment/ Action |
|---|---|---|---|---|
| New customer | Likely | Moderate | Medium | Standard ID check = CDD:<br>• Obtain and maintain correct and complete information and documents<br>• Standard KYC<br>• Verification of information and documents<br>• Monitoring of transaction. |
| New customer who wants to carry out a large transaction | Likely | Moderate | Medium | Standard ID check = CDD:<br>• Obtain and maintain correct and complete information and documents<br>• Standard KYC<br>• Verification of source of fund<br>• Verification of information and documents<br>• Monitoring of transaction. |
| Customer or group of customers making lots of transactions to the same individual or group | Likely | Moderate | Medium | Standard ID check = CDD:<br>• Obtain and maintain correct and complete information and documents<br>• Standard KYC<br>• Verification of source of fund<br>• KYC of BO (if any)<br>• Verification of information and documents<br>• Monitoring of transaction. |
| Customer who has a business which involves large amounts of cash | Very Likely | Minor | Medium | Standard ID check = CDD:<br>• Obtain and maintain correct and complete information and documents<br>• Standard KYC<br>• Verification of source of fund<br>• Verification of information |

| | | | | |
|---|---|---|---|---|
| | | | | and documents<br>• Monitoring of transaction. |
| Customer whose identification is difficult to check | Unlikely | Moderate | Low | Standard ID check = CDD:<br>• Obtain and maintain correct and complete information and documents<br>• Standard KYC<br>• Verification of information and documents<br>• Monitoring of transaction. |
| Customer who brings in large amounts of used notes and/or small denominations | Unlikely | Moderate | Low | Standard ID check = CDD:<br>• Obtain and maintain correct and complete information and documents<br>• Standard KYC<br>• Verification of information and documents<br>• Monitoring of transaction. |
| Customer who has significant and unexplained geographic distance between the institution and the location of the customer | Very Likely | Moderate | High | Standard + additional ID check = EDD:<br>Customer Due Diligence:<br>• Obtain and maintain correct and complete information and documents |
| | | | | • Standard KYC<br>• Verification of source of fund<br>• Verification of information and documents<br>• Monitoring of transaction.<br>Enhanced Due Diligence:<br>• Additional information and documents to be collected and updated i.e. Occupation, Wealth Statement, explanation of transaction etc.<br>• Transaction to be done after getting prior permission from top management. |
| Customer who has frequent and unexplained movement of accounts to different institutions | Likely | Minor | Low | Standard ID check = CDD:<br>• Obtain and maintain correct and complete information and documents<br>• Standard KYC<br>• Verification of information and documents<br>• Monitoring of transaction. |
| Customer who has frequent and unexplained movement of funds between institutions in various geographic locations | Unlikely | Minor | Low | Standard ID check = CDD:<br>• Obtain and maintain correct and complete information and documents<br>• Standard KYC |

| | | | | |
|---|---|---|---|---|
| | | | | • Verification of information and documents<br>• Monitoring of transaction. |
| Non- resident customer | Unlikely | Minor | Low | Standard ID check = CDD:<br>• Obtain and maintain correct and complete information and documents<br>• Standard KYC<br>• Verification of information and documents<br>• Information to be collected as per the directives of Guidelines of for Foreign Exchange Transactions.<br>• Monitoring of transaction. |
| Corporate customer whose ownership structure is unusual and excessively complex | Likely | Moderate | Medium | Standard ID check = CDD:<br>• Obtain and maintain correct and complete information and documents<br>• Standard KYC<br>• KYC of BO (if any)<br>• Verification of source of fund<br>• Verification of information and documents<br>• Monitoring of transaction. |
| Customers that are politically exposed persons (PEPs) or influential persons (IPs) or head of international organizations and their family members and close associates | Very Likely | Moderate | High | Standard + additional ID check = EDD:<br>Customer Due Diligence:<br>• Obtain and maintain correct and complete information and documents<br>• Standard KYC<br>• Verification of source of fund<br>• Verification of information and documents<br>• Monitoring of transaction.<br>Enhanced Due Diligence:<br>• Additional information and documents to be collected and updated i.e. Occupation, Wealth Statement, explanation of transaction etc.<br>• Transaction to be done after getting prior permission from top management.<br>• KYC of BO (if any)<br>• Regular monitoring of transaction.<br>• Information to be collected as per the directives of |

| | | | | |
|---|---|---|---|---|
| | | | | Guidelines of for Foreign Exchange Transactions. |
| Customer submits account documentation showing an unclear ownership structure | Unlikely | Minor | Low | Standard ID check = CDD:<br>• Obtain and maintain correct and complete information and documents<br>• Standard KYC<br>• KYC of BO (if any)<br>• Verification of source of fund<br>• Verification of information and documents<br>• Monitoring of transaction. |
| Customer opens account in the name of his/her family member who intends to credit large amount of deposits not consistent with the known sources of legitimate family income | Likely | Moderate | Medium | Standard ID check = CDD:<br>• Obtain and maintain correct and complete information and documents<br>• Standard KYC<br>• KYC of BO (if any)<br>• Verification of source of fund<br>• Verification of information and documents<br>• Monitoring of transaction. |
| Customer comes with premature encashment of fixed deposit | Unlikely | Minor | Low | Standard ID check = CDD:<br>• Obtain and maintain correct and complete information and documents |
| | | | | • Standard KYC<br>• KYC of BO (if any)<br>• Verification of source of fund<br>• Verification of information and documents<br>• Monitoring of transaction. |
| Customer generally tries to convince for cash deposit but insists for financial instrument while withdrawing the deposit | Unlikely | Minor | Low | Standard ID check = CDD:<br>• Obtain and maintain correct and complete information and documents<br>• Standard KYC<br>• KYC of BO (if any)<br>• Verification of source of fund<br>• Transaction to be done through bank instrument<br>• Verification of information and documents<br>• Monitoring of transaction. |
| Customer who wants to settle his loan early | Likely | Moderate | Medium | Standard ID check = CDD:<br>• Obtain and maintain correct and complete information and documents |

| | | | | |
|---|---|---|---|---|
| | | | | • Standard KYC<br>• Verification and update of source of fund<br>• Verification of information and documents<br>• Monitoring of transaction. |
| Government employee having several large amounts of fixed deposit accounts | Likely | Moderate | Medium | Standard ID check = CDD:<br>• Obtain and maintain correct and complete information and documents<br>• Standard KYC<br>• Verification and update of source of fund<br>• Verification of information and documents<br>• Monitoring of transaction. |
| Customer who has an unusual or excessively nervous demeanor | Likely | Minor | Low | Standard ID check = CDD:<br>• Obtain and maintain correct and complete information and documents<br>• Standard KYC<br>• KYC of BO (if any)<br>• Verification of source of fund<br>• Verification of information and documents<br>• Monitoring of transaction. |
| Customer who discusses your record-keeping or reporting duties with the apparent intention of avoiding them | Very Likely | Minor | Medium | Standard ID check = CDD:<br>• Obtain and maintain correct and complete information and documents<br>• Standard KYC<br>• KYC of BO (if any)<br>• Verification of source of fund<br>• Verification of information and documents<br>• Monitoring of transaction. |
| Customer who threatens an employee in an effort to discourage required record-keeping or reporting | Likely | Minor | Low | Standard ID check = CDD:<br>• Obtain and maintain correct and complete information and documents<br>• Standard KYC<br>• KYC of BO (if any)<br>• Verification of source of fund<br>• Verification of information and documents<br>• Monitoring of transaction. |
| Customer who is reluctant to proceed with a transaction after being told it must be recorded | Likely | Minor | Low | Standard ID check = CDD:<br>• Obtain and maintain correct and complete information |

| | | | | |
|---|---|---|---|---|
| | | | | and documents<br>• Standard KYC<br>• KYC of BO (if any)<br>• Verification of source of fund<br>• Verification of information and documents<br>• Monitoring of transaction. |
| Customer who 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 | Likely | Moderate | Medium | Standard ID check = CDD:<br>• Obtain and maintain correct and complete information and documents<br>• Standard KYC<br>• KYC of BO (if any)<br>• Verification of source of fund<br>• Verification of information and documents<br>• Monitoring of transaction. |
| Agent, attorney or financial advisor who acts for another person without proper documentation such as a power of attorney | Unlikely | Minor | Low | Standard ID check = CDD:<br>• Obtain and maintain correct and complete information and documents<br>• Standard KYC<br>• Legal status of agent, attorney or financial advisor to be verified<br>• Verification of source of fund<br>• Verification of information and documents<br>• Monitoring of transaction. |
| Customer who furnishes unusual or suspicious identification documents and is unwilling to provide personal data | Likely | Moderate | Medium | Standard ID check = CDD:<br>• Obtain and maintain correct and complete information and documents<br>• Standard KYC<br>• KYC of BO (if any)<br>• Verification of source of fund<br>• Verification of information and documents<br>• Monitoring of transaction. |
| Business customer who is reluctant to reveal details about the business activities or to provide financial statements or documents about a related business entity | Unlikely | Minor | Low | Standard ID check = CDD:<br>• Obtain and maintain correct and complete information and documents<br>• Standard KYC<br>• KYC of BO (if any)<br>• Verification of source of fund<br>• Verification of information |

| | | | | |
|---|---|---|---|---|
| | | | | and documents<br>• Monitoring of transaction. |
| Customer who opens several accounts in or more names, then makes several cash deposits under the reporting threshold | Likely | Moderate | Medium | Standard ID check = CDD:<br>• Obtain and maintain correct and complete information and documents<br>• Fund to be collected through bank instrument.<br>• Standard KYC<br>• KYC of BO (if any)<br>• Verification of source of fund<br>• Verification of information and documents<br>• Monitoring of transaction. |
| Customer who conducts large cash transactions at different branches on the same day, or orchestrates persons to do so in his/her behalf | Unlikely | Minor | Low | Standard ID check = CDD:<br>• Obtain and maintain correct and complete information and documents<br>• Standard KYC<br>• KYC of BO (if any)<br>• Verification of source of fund<br>• Verification of information and documents<br>• Monitoring of transaction. |
| Customer whose financial statement makes representations that do not conform to accounting principles | Likely | Moderate | Medium | Standard ID check = CDD:<br>• Obtain and maintain correct and complete information and documents<br>• Standard KYC<br>• KYC of BO (if any)<br>• Verification of information and documents<br>• Monitoring of transaction. |
| Customer who suddenly pays off a large problem loan with no plausible explanation of source of funds | Likely | Moderate | Medium | Standard ID check = CDD:<br>• Verification and update of source of fund<br>• Update of KYC |
| Customer who purchases certificates of deposit and uses them as collateral for a loan | Unlikely | Minor | Low | Standard ID check = CDD:<br>• Obtain and maintain correct and complete information and documents<br>• Standard KYC<br>• KYC of BO (if any)<br>• Verification of utilization of fund<br>• Verification of information and documents<br>• Monitoring of transaction. |
| Business customer who presents financial statements noticeably | Likely | Moderate | Medium | Standard ID check = CDD:<br>• Obtain and maintain correct |

| | | | | |
|---|---|---|---|---|
| different from those of similar businesses | | | | and complete information and documents<br>• Standard KYC<br>• KYC of BO (if any)<br>• Verification of source of fund<br>• Verification of information and documents<br>• Monitoring of transaction. |
| Large business presents financial statements that are not prepared by an accountant | Likely | Moderate | Medium | Standard ID check = CDD:<br>• Obtain and maintain correct and complete information and documents<br>• Standard KYC<br>• KYC of BO (if any)<br>• Verification of source of fund<br>• Verification of information and documents<br>• Monitoring of transaction. |

## Risk group: Products and services

| Risk | Likelihood | Impact | Risk score | Treatment/ Action |
|---|---|---|---|---|
| Prioritized or privileged financial service | Likely | Moderate | Medium | Standard ID check = CDD:<br>• Obtain and maintain correct and complete information and documents<br>• Standard KYC<br>• KYC of BO (if any)<br>• Verification of information and documents<br>• Monitoring of transaction. |
| Anonymous transaction | Unlikely | Major | Medium | • No transaction to be done. |
| Non face to face business relationship or transaction | Unlikely | Minor | Low | • Identify ML & TF risk<br>• Policy to be prepared to reduce risk<br>• Review the policy time to time. |
| Payment received from unknown or unrelated third parties | Unlikely | Minor | Low | • Identify ML & TF risk<br>• Monitoring of transaction. |
| Any new product and services developed | Unlikely | Minor | Low | • Identify ML & TF risk<br>• Policy to be prepared to reduce risk<br>• Review the policy time to time. |
| Service to walk-in customers | Unlikely | Minor | Low | Standard ID check = CDD:<br>• Obtain and maintain correct and complete information and documents<br>• Short KYC<br>• KYC of BO (if any) |

| | | | | |
|---|---|---|---|---|
| | | | | • Verification of information and documents |
| Syndicate financing | Likely | Major | High | Standard + additional ID check = EDD:<br>Customer Due Diligence:<br>• Obtain and maintain correct and complete information and documents<br>• Standard KYC<br>• Verification of information and documents<br>Enhanced Due Diligence:<br>• Additional information and documents to be collected and updated<br>• Vetting of syndicated documents<br>• Verification fund utilization<br>• Transaction to be done after getting prior permission from top management.<br>• Regular monitoring of transaction. |
| Receivable financing | Unlikely | Major | Medium | Standard ID check = CDD:<br>• Obtain and maintain correct and complete information and documents<br>• Standard KYC<br>• KYC of BO (if any)<br>• Verification of source of fund<br>• Verification of documents of receivables<br>• Monitoring of transaction. |
| Home equity and loan against FDR/deposits/financial instruments | Likely | Moderate | Medium | Standard ID check = CDD:<br>• Obtain and maintain correct and complete information and documents<br>• Standard KYC<br>• KYC of BO (if any)<br>• Monitoring of utilization of fund. |
| Sale and lease back facility | Likely | Major | High | Standard + additional ID check = EDD:<br>Customer Due Diligence:<br>• Obtain and maintain correct and complete information and documents<br>• Standard KYC<br>• Verification of information and documents<br>Enhanced Due Diligence:<br>• Additional information and |

| | | | | |
|---|---|---|---|---|
| | | | | documents to be collected and updated<br>• Ownership of the assets to be verified<br>• Verification of fund utilization<br>• Transaction to be done after getting prior permission from top management.<br>• Regular monitoring of transaction. |
| Working capital finance | Very Likely | Minor | Medium | Standard ID check = CDD:<br>• Obtain and maintain correct and complete information and documents<br>• Standard KYC<br>• Monitoring of utilization of fund. |
| Short term loan to different business concern to meet urgent fund requirement for any interim period | Likely | Moderate | Medium | Standard ID check = CDD:<br>• Obtain and maintain correct and complete information and documents<br>• Standard KYC<br>• Monitoring of utilization of fund. |
| SME tailored loan | Likely | Moderate | Medium | Standard ID check = CDD:<br>• Obtain and maintain correct and complete information and documents<br>• Standard KYC<br>• KYC of BO (if any)<br>• Monitoring of utilization of fund. |

## Risk group: Business practice/delivery methods or channels

| Risk | Likelihood | Impact | Risk score | Treatment/ Action |
|---|---|---|---|---|
| | | | | |
| Direct to the customer | Very Likely | Minor | Medium | Standard ID check = CDD:<br>• Obtain and maintain correct and complete information and documents<br>• Standard KYC<br>• KYC of BO (if any)<br>• Verification of source of fund<br>• Verification of information and documents<br>• Monitoring of transaction. |
| Online/internet | Very Likely | Minor | Medium | Standard ID check = CDD:<br>• Obtain and maintain correct |

| | | | | |
|---|---|---|---|---|
| | | | | and complete information and documents<br>• Standard KYC<br>• KYC of BO (if any)<br>• Verification of source of fund<br>• Verification of information and documents<br>• Monitoring of transaction. |
| Phone | Unlikely | Minor | Low | Standard ID check = CDD:<br>• Obtain and maintain correct and complete information and documents<br>• Standard KYC<br>• KYC of BO (if any)<br>• Verification of source of fund<br>• Verification of information and documents<br>• Monitoring of transaction. |
| Fax | Likely | Minor | Low | Standard ID check = CDD:<br>• Obtain and maintain correct and complete information and documents<br>• Standard KYC<br>• KYC of BO (if any)<br>• Verification of source of fund<br>• Verification of information and documents<br>• Monitoring of transaction. |
| E-mail | Very Likely | Minor | Medium | Standard ID check = CDD:<br>• Obtain and maintain correct and complete information and documents<br>• Standard KYC<br>• KYC of BO (if any) |
| | | | | • Verification of source of fund<br>• Verification of information and documents<br>• Monitoring of transaction. |
| Third-party, agent or broker | Likely | Moderate | Medium | Standard ID check = CDD:<br>• Obtain and maintain correct and complete information and documents<br>• Standard KYC<br>• KYC of BO (if any)<br>• Verification of source of fund<br>• Verification of legal status of |

| | | | | |
|---|---|---|---|---|
| | | | | third-party, agent or broker<br>• Verification of information and documents<br>• Monitoring of transaction. |

## Risk group: Country/jurisdiction

| Risk | Likelihood | Impact | Risk score | Treatment/ Action |
|---|---|---|---|---|
| Country which is unidentified by credible sources as having significant level of corruption and criminal activity | Unlikely | Minor | Low | |
| Country subject to economic or trade sanctions | Unlikely | Minor | Low | |
| Country known to be tax haven and unidentified credible sources as providing funding or support for terrorist activities or that have designated terrorist organizations operating within their country | Unlikely | Minor | Low | |
| Country unidentified by FATF or FSRBs as not having adequate AML & CFT system | Unlikely | Minor | Low | |
| Country identified as designation of illicit financial flow | Unlikely | Minor | Low | |
| Branch in any land port, sea port city or any border area | Unlikely | Minor | Low | |

## Risk group: Regulatory risk

| Risk | Likelihood | Impact | Risk score | Treatment/ Action |
|---|---|---|---|---|
| Customer/beneficial owner identification and verification not done properly | Unlikely | Major | Medium | • Create awareness of employee<br>• Arrange training program regularly. |
| Failure to keep record properly | Unlikely | Major | Medium | • Create awareness of employee.<br>• Arrange training program regularly. |
| Failure to scrutinize staffs properly | Unlikely | Moderate | Low | • Verify employee through CMMS at the time of joining<br>• Maintain KYE |
| Failure to train staff adequately | Likely | Moderate | Medium | • Arrange training program regularly. |
| Not having an AML & CFT program | Unlikely | Moderate | Low | • Preparing AML & CFT program. |
| Failure to report suspicious transactions or activities | Unlikely | Major | Medium | • Strengthening the CCU<br>• Monitoring ML & TF issue. |
| Not submitting required report to BFI U regularly | Unlikely | Major | Medium | • Strengthening the CCU<br>• Monitoring report submission status regularly. |
| Not having an AML & CFT Compliance Officer | Unlikely | Moderate | Low | • Appoint an AML & CFT |

| | | | | |
|---|---|---|---|---|
| | | | | Compliance Officer. |
| Failure of doing Enhanced Due Diligence (EDD) for high risk customers (i.e., PEPs, IPs) | Likely | Moderate | Medium | • Create awareness of employee.<br>• Arrange training program regularly. |
| Not complying with any order for freezing or suspension of transaction issued by BFIU or BB | Unlikely | Major | Medium | • Maintain separate statement and monitoring the same regularly. |
| Not submitting accurate information or statement requested by BFIU or BB | Likely | Moderate | Medium | • Checking of information or statement by higher authority. |

## Section-4: Central Compliance Unit and its reporting

### 4.1 Establishment of Central Compliance Unit (CCU)

FFIL shall establish arrangement for internal monitoring and control through formation of a Central Compliance Unit (CCU) under the leadership of a high official at the Head Office.

CCU is authorized to adopt new member(s) if they think proper. The quorum for CCU meeting will be four members present in person for that meeting. The Member Secretary shall keep the meeting records in proper manner.

### 4.2 Responsibilities of CCU

CCU will prepare and issue instructions to be followed by the branches; 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 and terrorist financing. CCU shall be dedicated solely to the organization's related responsibilities and perform the compliance functions. The responsibilities of CCU include:

(i) Preparing an overall assessment report after evaluating the self assessment reports received from the branches and submitting it with comments and recommendations to the Managing Director on half yearly basis;
(ii) Preparing an assessment report on the basis of the submitted checklist of inspected branches by the Internal Compliance Department on that particular quarter;
(iii) Submitting reports to BFIU according to the guidelines issued by Bangladesh Financial Intelligence Unit (BFIU).

## 4.3 Self assessment

4.3.1 CCU shall introduce half yearly self assessment procedure that will assess how effectively the AML/CFT program is working. This procedure shall enable FFIL management to identify areas of risk or to assess the need for additional control mechanisms.

4.3.2 CCU shall prepare the self assessment report documenting the work performed; how it was controlled/supervised and the resulting findings, conclusions and recommendations.

4.3.3 Each branch will assess its AML/CFT activities covering the following areas on half yearly basis and submit the self assessment report to CCU within next 20 days:

- The percentage of officers/employees that received official training on AML/CFT;
- The awareness of the officers/employees about the internal AML/CFT policies,
- procedures and programs, and Bangladesh Financial Intelligence Unit (BFIU) instructions and guidelines;
- The arrangement of AML/CFT related meeting on regular interval;
- The effectiveness of the customer identification during opening an individual, corporate and other account;
- The risk categorization of customers by the branch;
- Regular update of customer profile upon reassessment;
- The monitoring of customers' transactions with their declared TP after categorizing the customers based on risk or transactions over specific limit;
- Identification of Suspicious Transaction Reports (STRs);
- The maintenance of a separate file containing ML PA, Circulars, Training Records, Reports and other AML related documents and distribution of those among all employees;
- The measures taken by the branch during opening of account of PEPs;
- Consideration of UN Sanction List while conducting any business.
- The compliance with AML/CFT weaknesses/irregularities, as the bank's Head Office and Bangladesh Financial Intelligence Unit (BFIU) inspection report mentioned.

## 4.4 Independent testing procedure

4.4.1 FFIL internal compliance department shall perform the independent testing procedure covering the following areas and submit a report to the Board Audit Committee on annual basis:

- Branch Compliance Unit/BAMLCO
- Knowledge of officers/employees on AML/CFT issues
- Customer Identification (KYC) process
- Branch's receipt of customers' expected transaction profile and monitoring

- Process and action to identify Suspicious Transaction Reports (STRs)
- Regular submission of reports to CCU
- Proper record keeping
- Overall AML related activities by the branch

4.4.2 The tests may include interviews with employees handling transactions and interviews with their supervisors to determine their knowledge and compliance with the financial institution's anti-money laundering procedures along with the following:

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

**Section-5: Appointment as CAMLCO & DCAMLCO**

The FFIL management shall designate two employees as CAMLCO & DCAMCO allowing authority to implement and enforce corporate-wide AML/CFT policies, procedures and measures in the company. CAMLCO will directly report to the Managing Director for his/her responsibility. CAMLCO will also be responsible to coordinate and monitor day-to-day compliance with applicable AML/CFT related laws, rules and regulations as well as with its internal policies, practices, procedures and controls.

**5.1 Position of CAMLCO**

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

**5.2 Qualification and experience of CAMLCO**

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

## 5.3 Responsibilities of CAMLCO

The major responsibilities of a CAMLCO are as follows:

- Chairs the CCU meeting;
- Monitors, reviews and coordinates application and enforcement of the financial institution's compliance policies including AML/CFT Compliance Policy. This will include an AML/CFT risk assessment, practices, procedures and controls for account opening, KYC procedures and ongoing account/transaction monitoring for detecting suspicious transaction/account activity, and a written AML/CFT training plan;
- Monitors changes of laws/regulations and directives of Bangladesh Financial Intelligence Unit (BFIU) and revise its internal policies accordingly;
- Responds to compliance questions and concerns of the staff and advise regional offices/branches/units and assist in providing solutions to potential issues involving compliance and risk;
- Ensures that AML/CFT policy is complete and up-to-date, maintains ongoing awareness of new and changing business activities and products and identifies potential compliance issues that should be considered by FFIL;
- Develops the compliance knowledge of all staff, especially the compliance personnel and conduct training courses in the institution in this regard;
- Develops and maintains ongoing relationships with regulatory authorities, external and internal auditors, regional/branch/unit heads and compliance resources to assist in early identification of compliance issues;
- Assists in review of control procedures in FFIL to ensure legal and regulatory compliance and in the development of adequate and sufficient testing procedures to prevent and detect compliance lapses;
- Monitors the business through self-testing for AML/CFT compliance and take any required corrective action;
- Determines the structure and resource levels of AML;
- Ensures resources are deployed effectively to support the Business in mitigating AML risks;
- Drives communication to the Board / CEO/ Audit Committee and other stakeholders with respect to issues concerning AML;
- Represents AML at Board, Management Committees and at senior corporate level as appropriate;
- Maintains relationships to external auditors, regulatory and other regulatory bodies;
- Controls, manages and administers AML's budget and resources planning processes;
- Is responsible for AML systems, technology, AML Risk Analysis, MIS and operations;
- Manages the Suspicious Transaction Report /Suspicious Activity Report process:

- ❖ reviewing transactions referred by divisional, regional, branch or unit compliance officers as suspicious;
- ❖ reviewing the transaction monitoring reports (directly or together with account management personnel);
- ❖ ensuring that internal Suspicious Activity Reports (SARs):
  - are prepared when appropriate;
  - reflect the uniform standard for "suspicious activity involving possible money laundering or terrorist financing" established in its policy;
  - are accompanied by documentation of the branch's decision to retain or terminate the account as required under its policy;
  - are advised to other branches of the institution who are known to have a relationship with the customer;
  - are reported to the Chief Executive Officer, and the Board of Directors of the institution when the suspicious activity is judged to represent significant risk to the institution, including reputation risk .
- ❖ ensuring that a documented plan of corrective action, appropriate for the seriousness of the suspicious activity, be prepared and approved by the branch manager;
- ❖ maintaining a review and follow up process to ensure that planned corrective action, including possible termination of an account, be taken in a timely manner;
- ❖ managing the process for reporting suspicious activity to BFIU after appropriate internal consultation;

### 5.4 Qualification and experience of Deputy CAMLCO:

The Deputy Chief AML/CFT Compliance Officer should have a minimum of five years of working experience in banks and financial institutions.

### 5.5 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 BFIU on Institution's behalf.
- Controlling flow of information to BAMLCO for required actions (if any)

## Section-6: Branch Anti Money Laundering Officer (BAMLCO)

FFIL shall appoint BAMLCO at each of their branches. BAMLCO will be the second man of a branch and have minimum three year experience in related field. The responsibilities of a BAMLCO will be as follows:

- Have a direct reporting line to Head of CCU.
- Manage the transaction monitoring process and report any suspicious activity to Branch Manager, and if necessary to the CAMLCO
- Are responsible for the implementation of the applicable Policies on AML & KYC.
- Provide training to Branch staff.
- Ensure that guidelines and procedures are in line with Anti Money Laundering laws / regulations and the applicable regulations of Bangladesh Financial Intelligence Unit (BFIU).
- Are the primary point of contact with regulators and law enforcement authorities
- Are responsible for the AML Risk Analysis
- Communicate to all staff in case of any changes in national or its own policy.
- Are responsible for the implementation of adequate monitoring – research /surveillance tools
- Track and follow up on the conditions that have been imposed as part of the KYC approval
- Develop and maintain procedures and systems to ensure that unusual and suspicious transactions are reported to CAMLCO.
- Develop and carry out adequate controls to ensure that all applicable legal and regulatory AML requirements are being adhered to.
- Sign-off in the New Product Approval and Smart sourcing process where appropriate.
- Submit branch returns to CAMLCO timely.

## Section-7: Responsibilities of other employees

The table below details the individual responsibilities of the FFIL employees:

| **Function** | **Role / Responsibilities** |
|---|---|
| Staff Responsible for account opening | • Perform due diligence on prospective clients prior opening an account<br>• Be diligent regarding the identification (s) of account holder and the transactions relating to the account<br>• Ensure all required documentation is completed satisfactorily<br>• Complete the KYC Profile for the new customer<br>• Ongoing monitoring of customers KYC profile and transaction activity<br>• Escalate any suspicion to the Supervisor, Branch Manager and BAMLCO |

| | |
|---|---|
| Customer Service Officer | • Support the Account Officer in any of the above roles<br>• Perform the Account Officer roles in their absence |
| Operations Staff | • Ensure that all control points are completed prior to transaction monitoring<br>• Be diligent on transaction trends for clients<br>• Update customer transaction profiles in the ledger/system |
| Branch Manager (Unit Head) | • Ensure that the program is effective within the branch/unit<br>• First point of contact for any issues |
| Risk Management /Credit Officer/ Internal Control Officer | • Perform Risk Assessment for the Business<br>• Perform periodic Quality Assurance on the program in the unit<br>➢ Communicate updates in laws and internal policies |
| Operations & Technology Manager | ➢ Ensures that the required reports and systems are in place to maintain an effective program |
| Controller of Branches | ➢ Overall responsibility to ensure that the branches have an AML program in place and that it is working effectively |
| Managing Director | ➢ Overall responsibility to ensure that the Business has an AML program in place and it is working effectively |

## Section-8: Money Laundering-training and awareness

### 8.1 Overview

FFIL shall take reasonable care to provide appropriate anti-money laundering training on an ongoing basis for its employees who handle, or are managerially responsible for the handling of, transactions which may involve money laundering. All relevant staff should be educated in the process of the "Know Your Customer" requirements for money laundering and terrorist financing prevention purposes. The training in this respect should cover not only the need to know the true identity of the customer but also, where a business relationship is being established, the need to know enough about the type of business activities expected in relation to that customer at the outset to know what might constitute suspicious activity at a future date. Relevant staff should be alert to any change in the pattern of a customer's transactions of circumstances that might constitute criminal activity. FFIL shall provide initial training which:

- deals with the law on money laundering, and the responsibilities of staff;
- is applicable to all staff who handle, or are managerially responsible for the handling of, transactions which may involve money laundering and
- should be customer focused, and takes place with sufficient frequency (within a minimum period of 48 months) and ensure that it is given to all of the staff referred to in the above sub-para.

The training shall also include the following:

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

### 8.2 Specific job training

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

#### 8.2.1 New employees

A general appreciation of the background to money laundering and terrorist financing, and the subsequent need for reporting any suspicious transactions should

be provided to all new employees who are likely to be dealing with customers or their transactions, irrespective of the level of seniority. They should be made aware of the importance placed on the reporting of suspicions by the organization, that there is a legal requirement to report, and that there is a personal statutory obligation to do so.

### 8.2.2 Customer service/Relationship Managers

Executives who are dealing directly with the public are the first point of contact with potential money launderers and terrorist financiers and their efforts are vital to the organization's strategy in the fight against money laundering and terrorist financing. They must be made aware of their legal responsibilities and should be made aware of the organization's reporting system for such transactions. Training should be provided on factors that may give rise to suspicions and on the procedures to be adopted when a transaction is deemed to be suspicious. It is vital that 'front-line' staffs are made aware of the organization's policy for dealing with non-regular (walk-in) customers particularly where large transactions are involved, and the need for extra vigilance in these cases.

### 8.2.3 Processing (Back Office) employees

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

### 8.2.4 Credit Officers

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

### 8.2.5 Audit and compliance employees

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

### 8.2.6 Senior Management/Operations Supervisors and Managers

A higher level of instruction covering all aspects of money laundering and terrorist financing prevention procedures should be provided to those with the responsibility

for supervising or managing staff. This will include the offences and penalties arising from the laws for non-reporting and for assisting money launderers and terrorist financers; internal reporting procedures and the requirements for verification of identity and the retention of records.

### 8.2.7 Senior Management and Board of Directors

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

### 8.2.8 AML/CFT Compliance Officer

The AML/CFT Compliance Officer should receive in depth training on all aspects of the Money Laundering and Terrorist Financing Prevention Legislation, Bangladesh Financial Intelligence Unit (BFIU) directives and internal policies. In addition, the AML/CFT Compliance Officer will require extensive instructions on the validation and reporting of suspicious transactions and on the feedback arrangements, and on new trends and patterns of criminal activity.

## 8.3 The Combating Terrorism (Amendment) Act, 2012

It should be noted that any training given on anti money laundering must include the subject of the Combating Terrorism (Amendment) Act, 2012, and how this now covers all financial crime, however small.

A successful defense, under the Combating Terrorism (Amendment) Act, 2012, on the part of a member of staff of not having been trained to recognize and report suspicions, will leave the firm liable to prosecution for breach of the Regulations.

Not knowing the policies or procedures is not a defense. The regulations have implemented an 'ought' to know stance, and therefore all staff, referred to above must be trained.

## 8.4 Training procedures

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

- Identify the issues that must be communicated and decide how best to do this e.g. sometimes, e-learning can effectively do the job, sometimes classroom training is the best option.
- Identify the audience by functional area as well as level of employee/management. This should be accompanied by a quick "why are they here" assessment. New hires should receive training different from that given to veteran employees.

- Determine the needs that are being addressed; e.g. uncovered issues by audits or examinations, created by changes to systems, products or regulations.
- Determine who can best develop and present the training program.
- Create a course abstract or curriculum that addresses course goals, objectives and desired results. Be sure to identify who the audience should be and how the material will be presented.
- Establish a training calendar that identifies the topics and frequency of each course.
- Course evaluation shall be done to evaluate how well the message is received; copies of the answer key should be made available. Similarly, in case of a case study used to illustrate a point, provide detailed discussion of the preferred course of action.
- Track Attendance by asking the attendees to sign in. Employee who shall remain absent without any reason may warrant disciplinary action and comments in employee's personal file.

### 8.5 Refresher training

In addition to the above compliance requirements, training are to be tailored to the needs of specialized areas of the FFIL business. It will also be necessary to keep the content of training programs under review and to make arrangements for refresher training at regular intervals i.e. at least bi-annually to ensure that staff does not forget their responsibilities and to reflect individual circumstances, possibly in conjunction with compliance monitoring. Training should be conducted ongoing basis, incorporating trends and developments in FFIL business risk profile, as well as changes in the legislation. Training on new money laundering and terrorist financing schemes and typologies are of the utmost importance when reviewing policies and controls and designing monitoring mechanisms for suspicions activity.

### 8.6 In practice

Records regarding Executives' training shall be maintained by CAMLCO through signature on a register. These records shall assist in the completion of the annual report to be submitted to the Board of Directors.

#### 8.6.1 Who should be trained and when?

It is mandatory for all employees that handles, or is managerially responsible for the handling of, transactions which may involve money laundering, and who may act for customers who are categorized as risk levels 1, 2 or 3 to be trained to understand the procedures in place within FFIL to minimize the risk of money laundering.

#### 8.6.2 What should training cover?

Training provided should enable all employees with the responsibility for handling transactions, adequate awareness of and to observe and assess the information that is required for them to judge whether a transaction or instruction is suspicious in the circumstances.

The frequency and nature of induction and repeat training should take into account the expected skills of the staff concerned, the nature of the business, transactions and the means of delivery, i.e. whether face-to-face or remote.

In keeping up-to-date with changes, sanctions lists and industry news, the Responsible Officer should notify staff of material changes through additional 'ad hoc' training or in the form of news bulletins, for example. It is of particular importance that Compliance and Internal Audit staff, at least, is kept abreast of changes to regulations so that appropriate monitoring of the business can be implemented.

### 8.6.3 Training should be risk based

Training should take a risk based approach by including consideration of business carried out by the Company. Staff should be advised how to handle such situations so that appropriate emphasis is placed on the need to check on the sources of funds.

It is of paramount importance that the message given to staff during training is: "There are no degrees of suspicion; you are either suspicious or you are not "when in any doubt, submit a suspicion report".

## 8.7 Independent audit function

### 8.7.1 Why the audit function is necessary

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

### 8.7.2 Why the audit function must be independent

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

### 8.7.3 Whom they report

The individuals conducting the audit should report directly to the board of directors/senior management.

### 8.7.4 The ways of performing audit function

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

### 8.7.5 Internal compliance department

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

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

### 8.7.6 External auditor

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

## Section-9: Customer Due Diligence

### 9.1 Know Your Customer program

The adoption of effective Know Your Customer (KYC) program is an essential part of financial institutions' risk management policies. Having sufficiently verified/corrected information about customers "Knowing Your Customer" (KYC) - and making use of that information underpins all AML/CFT efforts, and is the most effective defense against being used to launder the proceeds of crime. Keeping that in view, FFIL adopted adequate KYC program to minimize significant risks, especially legal and reputation risk. Sound KYC policies and procedures not only contribute to the FFIL's overall safety and soundness, they also protect the integrity of its system by reducing money laundering, terrorist financing and other related offences.

### 9.2 Know Your Customer procedure

Money Laundering Prevention Act, 2012 requires all reporting agencies to maintain correct and concrete information with regard to identity of its customer during the operation of their accounts. According to FATF recommendation where FFIL 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.

### 9.2.1 Nature of customer's business

When a business relationship is being established, the nature of the business that the customer expects to conduct with the institution should be ascertained at the outset to establish what might be expected later as normal activity. FFIL shall update this information as appropriate, and as opportunities arise. In line with that information FFIL shall judge whether a transaction carried out by its customers is or is not suspicious.

### 9.2.2 Identifying real person

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

### 9.2.3 Document is not enough

The best identification documents possible should be obtained from the prospective customer i.e. those that are the most difficult to obtain illicitly. No

single piece of identification can be fully guaranteed as genuine, or as being sufficient to establish identity so verification will generally be a cumulative process. The overriding principle is that FFIL must know who their customers are, and have the necessary documentary evidence to verify this. It should always be remembered that collection of document is not enough for KYC, identification of the customer is very important.

### 9.2.4 Who is a customer?

For the purpose of KYC Procedure a "Customer" is defined in AML Circular No. 24 dated March 03, 2010, as:

- any person or institution maintaining an account of any type with a bank or financial institution or having banking related business;
- the person or institution as true beneficial owner in whose favour the account is operated;
- the trustee, intermediary or true beneficial owner of the transaction of the accounts operated by the trust and professional intermediaries (such as lawyer/law firm, chartered accountant, etc) under the existing legal infrastructure;
- high value single transaction conducted in a single Demand Draft, Pay Order, Telegraphic Transfer by any person or institution or any person/institution involved in a financial transaction that may pose reputation and other risks to the institution. 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;

### 9.2.5 Customer acceptance policy

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

(i) No account should be opened in anonymous or fictitious name.
(ii) Parameters of risk perception should be clearly defined in terms of the source of fund, the nature of business activity, location of customer and his clients, mode of payments, volume of turnover, service offered, social and financial status etc. to categorize customers into different risk grades.
(iii) Documentation requirements and other information to be collected in respect of different categories of customers depending on perceived risk.

(iv) Not to open an account or close an account where FFIL is unable to apply appropriate customer due diligence measures i.e. FFIL is unable to verify the identity and/or obtain documents required as per the risk categorization due to non cooperation of the customer or non reliability of the data/information furnished to the financial institution. Decision by FFIL to close an account should be taken at a reasonably high level after giving due notice to the customer explaining the reasons for such a decision.

(v) Circumstances, in which a customer is permitted to act on behalf of another person/entity, should be clearly spelt out in conformity with the established law and practices of financial service as there could be occasions when an account is operated by a mandate holder or where an account is opened by an intermediary in fiduciary capacity.

(vi) Necessary checks before opening a new account to ensure that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations etc.

(vii) The status of a customer may change as relation with a customer progresses. The transaction pattern, volume of a customer's account may also change. With times an ordinary customer can turn into a risky one. To address this issue, customer acceptance policy should include measures to monitor customer's activities throughout the business relation.

(viii) The listed persons or institutions in UN Sanction list can't be the customer of FFIL.

(ix) For opening account in favor of Non residential citizen in Bangladesh FFIL should follow the instructions of Foreign Exchange Regulation Act, 1947.

### 9.2.6 Customer identification

Customer identification is an essential element of KYC standards. The customer identification process applies naturally at the outset of the relationship. To ensure that records remain up-to-date and relevant, there is a need for FFIL 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 FFIL becomes aware at any time that it lacks sufficient information about an existing customer, it should take steps to ensure that all relevant information is obtained as quickly as possible. Once verification of identity has been satisfactorily completed, no further evidence is needed to undertake subsequent transactions

### 9.2.7 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, in a non money-laundering context, to avoid breaches of UN or other international sanctions to which Bangladesh is a party. Where a passport is taken as evidence, the number, date and place of issuance should be recorded. The other main element in a person's identity is sufficient information about the nature of the business that the customer expects to undertake, and any expected or predictable, pattern of transactions. For some business these may be obvious, however, for more complex businesses this may not be the case. The extent of the description required will depend on the institution's own understanding of the applicant's business.

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

### 9.2.8 Individual customers

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

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

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

- Current valid passport;
- Valid driving license;
- National ID Card;
- Employer provided ID Card, bearing the photograph and signature of the

applicant;

Identification documents which do not bear photographs or signatures, or are easy to obtain, are normally not appropriate as sole evidence of identity, e.g. birth certificate, certificate from any local government organs, credit cards, non-Bangladeshi driving license. Any photocopies of documents showing photographs and signatures should be plainly legible. Where applicants put forward documents with which an institution is unfamiliar, either because of origin, format or language, the institution must take reasonable steps to verify that the document is indeed genuine, which may include contacting the relevant authorities or obtaining a notarized translation. Financial Institutions should also be aware of the authenticity of passports.

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

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

### 9.2.9 No face-to-face contact

Where there is no face-to-face contact, photographic identification would clearly be inappropriate procedures to identify and authenticate the customer. FFIL 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. FFIL should not allow non face to face contact to a resident in establishing relationship.

### 9.2.10 Appropriateness of documents

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

### 9.2.11 Joint accounts

In respect of joint accounts where the surname and/or address of the account holders differ, the name and address of all account holders, not only the first named, should

normally be verified in accordance with the procedures set out above.

### 9.2.12 Change in address or other details

Any subsequent change to the customer‘s name, address, or employment details of which FFIL becomes aware should be recorded as part of the Know Your Customer process. Generally this would be undertaken as part of good business practice and due diligence but also serves for money laundering prevention.

### 9.2.13 Record keeping

All documents collected or gathered 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. Institutions which regularly conduct one-off transactions, should record the details in a manner which allows cross reference to transaction records.

### 9.2.14 Introducer

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

### 9.2.15 Persons without standard identification documentation

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

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

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

### 9.2.16 Minor

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

### 9.2.17 Corporate bodies and other entities

Because of the difficulties of identifying beneficial ownership, and the possible complexity of organization and structures, corporate entities and trusts are the most likely vehicles to be used for money laundering, particularly when a legitimate trading company is involved. Particular care should be taken to verify the legal existence of the applicant and to ensure that any person purporting to act on behalf of the applicant is authorized to do so. The principal requirement is to look behind a corporate entity to identify those who have ultimate control over the business and the company's assets, with particular attention being paid to any shareholders or others who exercise a significant influence over the affairs of the company. Enquiries should be made to confirm that the company exists for a legitimate trading or economic purpose, and that it is not merely a "brass plate company" where the controlling principals cannot be identified. Before a business relationship is established, measures should be taken by way of company search and/or other commercial enquiries to ensure that the applicant company has not been, or is not in the process of being, dissolved, and struck off, wound-up or terminated. In addition, if FFIL becomes aware of changes in the company structure or ownership, or suspicions are aroused by a change in the nature of business transacted, further checks should be made. No further steps to verify identity over and above usual commercial practice will normally be required where the applicant for business is known to be a company, or a subsidiary of a company, quoted on a recognized stock exchange.

The following documents should normally be obtained from companies:

- Certified copy of Certificate of Incorporation or equivalent, details of the registered office, and place of business;
- Certified copy of the Memorandum and Articles of Association, or by-laws of the client.
- Copy of the board resolution to open the account relationship and the empowering authority for those who will operate any accounts;
- Explanation of the nature of the applicant's business, the reason for the relationship being established, an indication of the expected turnover, the source of funds, and a copy of the last available financial statements where appropriate;
- Satisfactory evidence of the identity of each of the principal beneficial owners being any person holding 10% interest or more or with principal control over the company‘s assets and any person (or persons) on whose instructions the signatories on the account are to act or may act where such persons are not full time employees, officers or directors of the company;
- Satisfactory evidence of the identity of the account signatories, details of their relationship with the company and if they are not employees an explanation of the relationship. Subsequent changes to signatories must be verified;
- Copies of the list/register of directors.
- Where the business relationship is being opened in a different name from that of the applicant, the institution should also satisfy itself that the reason for using the second name makes sense. The following persons (i.e. individuals or legal entities) must also be identified in line with this part of the notes:
- All of the directors who will be responsible for the operation of the account / transaction.
- All the authorized signatories for the account/transaction.
- All holders of powers of attorney to operate the account/transaction.
- The beneficial owner(s) of the company
- The majority shareholders of a private limited company.

A letter issued by a corporate customer is acceptable in lieu of passport or other photo identification documents of their shareholders, directors and authorized signatories. Where the institution already knows their identities and identification records already accord with the requirements of these notes, there is no need to verify identity again. When authorized signatories change, care should be taken to ensure that the identities of all current signatories have been verified. In addition, it may be appropriate to make periodic enquiries to establish whether there have been any changes in directors/shareholders, or the nature of the business/activity being undertaken. Such changes could be significant in relation to potential money laundering activity, even though authorized signatories have not changed.

**9.2.18 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, FFIL 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.

**9.2.19 Partnerships and unincorporated businesses**

In the case of partnerships and other unincorporated businesses whose partners/directors are not known to the FFIL, the identity of all the partners or equivalent should be verified in line with the requirements for personal customers. Where a formal partnership agreement exists, a mandate from the partnership authorizing the opening of an account and conferring authority on those who will operate it should be obtained. Evidence of the trading address of the business or partnership should be obtained and a copy of the latest report and accounts (audited where applicable). An explanation of the nature of the business or partnership should be ascertained (but not necessarily verified from a partnership deed) to ensure that it has a legitimate purpose.

**9.2.20 Powers of Attorney/ Mandates to operate accounts**

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

**9.2.21 Timing and duration of verification**

The best time to undertake verification is prior to entry into the account relationship. Verification of identity should, as soon as is reasonably practicable, be completed before any transaction is completed. However, if it is necessary for sound business reasons to open an account or carry out a significant one-off transaction before verification can be completed, this should be subject to stringent controls which should ensure that any funds received are not passed to third parties. Alternatively, a senior member of staff may give appropriate authority. This authority should not be delegated, and should only be done in exceptional circumstances. Any such decision should be recorded in writing. Verification, once begun, should normally be pursued either to a satisfactory conclusion or to the point of refusal. If a prospective customer does not pursue an application, staff may (or may not) consider that this is itself suspicious.

## 9.3 Know Your Employee (KYE)

Institutions and businesses learn at great expense that an insider can pose the same ML/TF threat as a customer. It has become clear in the field that having co-equal programs to know your customer and to know your employee is essential. In an effort to identify and anticipate trouble before it costs time, money and reputation damage, FFIL shall look closely at the people inside their own organizations. Keeping that in mind, FFIL shall introduce a KYE program that will allow it to understand an employee's background, conflicts of interest and susceptibility to money laundering complicity. The program will perform the background screening of prospective and current employees, especially for criminal history, to keep out unwanted employees and identifying those to be removed.

## Section-10: Record keeping

### 10.1 Statutory requirement

According to Section 25(1) of Money Laundering Prevention Act, 2012 (Amended 2015), FFIL shall retain correct and full records of customers' identification and transactions while operating an account of a customer. Again, according to FATF recommendation no. 11 FFIL shall maintain, for at least five years, all necessary records on transactions, both domestic and international, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved, if any) so as to provide, if necessary, evidence for prosecution of criminal activity. The records prepared and maintained by FFIL on its customer relationship and transactions should be such that:

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

Records relating to verification of identity will generally comprise:

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

Records relating to transactions will generally comprise:

- details of personal identity, including the names and addresses, etc. pertaining to:
  - the customer;
  - the beneficial owner of the account or product;
  - the non-account holder conducting any significant one-off transaction;
  - any counter-party;
- details of transaction including:
  - nature of such transactions;
  - volume of transactions customer's instruction(s) and authority(ies);

- source(s) of funds;
- destination(s) of funds;
- book entries;
- custody of documentation;
- date of the transaction;
- form in which funds are offered and paid out.
- parties to the transaction
- identity of the person who conducted the transaction on behalf of the customer

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

- closing of an account
- providing of any financial services
- carrying out of the one-off transaction, or the last in a series of linked one-off transactions; or
- ending of the business relationship; or
- commencement of proceedings to recover debts payable on insolvency.

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

**10.2 Retrieval of records**

To satisfy the requirements of the law and to meet the purpose of record keeping, it is important that records are capable of retrieval without undue delay. It is not necessary to retain all the documents relating to customer identity and transaction physically at the premises of the branch of FFIL, provided that they have reliable procedures for keeping the hard copy at a central archive, holding records in electronic form, and that can be reproduced and recollected without undue delay. It is not always necessary to retain documents in their original hard copy form, provided that FFIL has reliable procedures for holding records in microchips or electronic form, as appropriate, and that these can be reproduced without undue delay. In addition, FFIL may rely on the records of a third party, such as a bank or clearing house in respect of details of payments made by customers. However, the primary requirement is on FFIL itself and the onus is thus on the business to ensure that the third party is willing and able to retain and, if asked to, produce copies of the records required. However, the record requirements are the same regardless of the format in which they are kept or whether the transaction was undertaken by paper or electronic means. Documents held centrally must be capable of distinguishing between the transactions relating to different customers and of identifying where the transaction took place and in what form.

**10.3 STR and investigations**

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

- the date of submission and reference of the STR;
- the date and nature of the enquiry;
- the authority who made the enquiry, investigation and reference; and
- details of the account(s) involved.

**10.4 Branch level record keeping**

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

- Information regarding Identification of the customer,
- KYC information of a customer,
- Transaction report,
- Suspicious Transaction/Activity Report generated from the branch,
- Exception report,
- Training record,
- Return submitted or information provided to the Head Office or competent authority.

**10.5 Training records**

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

- details of the content of the training programs provided;
- the names of staff who have received the training;
- the date/duration of training;
- the results of any testing carried out to measure staffs understanding of the requirements; and
- an on-going training plan.

**10.6 Sharing of record/information of/to a customer**

Under MLPA 2012 ( Amended 2015), and ATA, 2009 (as amended in 2012), FFIL shall not share account related information to investigating authority i.e., Anti Corruption Commission or person authorized by ACC to investigate the said cases without having court order or prior approval from Bangladesh Financial Intelligence Unit(BFIU).

## Section-11: Suspicious transaction report

### 11.1 Definition of STR

Generally Suspicious Transaction Report (STR) 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.

According to Section (2)(z) of MLPA, 2012 (Amended 2015) "suspicious transaction" means such transactions which deviates from usual transactions; of which there is ground to suspect that,

- the property is the proceeds of an offence;
- it is financing to any terrorist activity, a terrorist group or an individual terrorist;
- which is, for the purposes of this Act, any other transaction or attempt of transaction delineated in the instructions issued by Bangladesh Financial Intelligence Unit (BFIU) from time to time.

In Anti Terrorism Act, 2009 (as amended in 2012), STR refers to the transaction that relates to financing for terrorism or terrorist individual or entities. One important thing is that according to the guidance notes issued by BB, FFIL need not to establish any proof of occurrence of a predicate offence; it is a must to submit STR only on the basis of suspicion.

### 11.2 Obligation and reasons for submission of STR

As per the Money Laundering Prevention Act, 2012, Anti Terrorism Act, 2009 (as amended in 2012) and Bangladesh Financial Intelligence Unit (BFIU) circulars issued from time to time, FFIL is obligated to submit STR to BB. STR is very crucial for the safety and soundness of FFIL and hence CCU of FFIL should consider the following while submitting STR to BB through using specified format (Appendix-B):

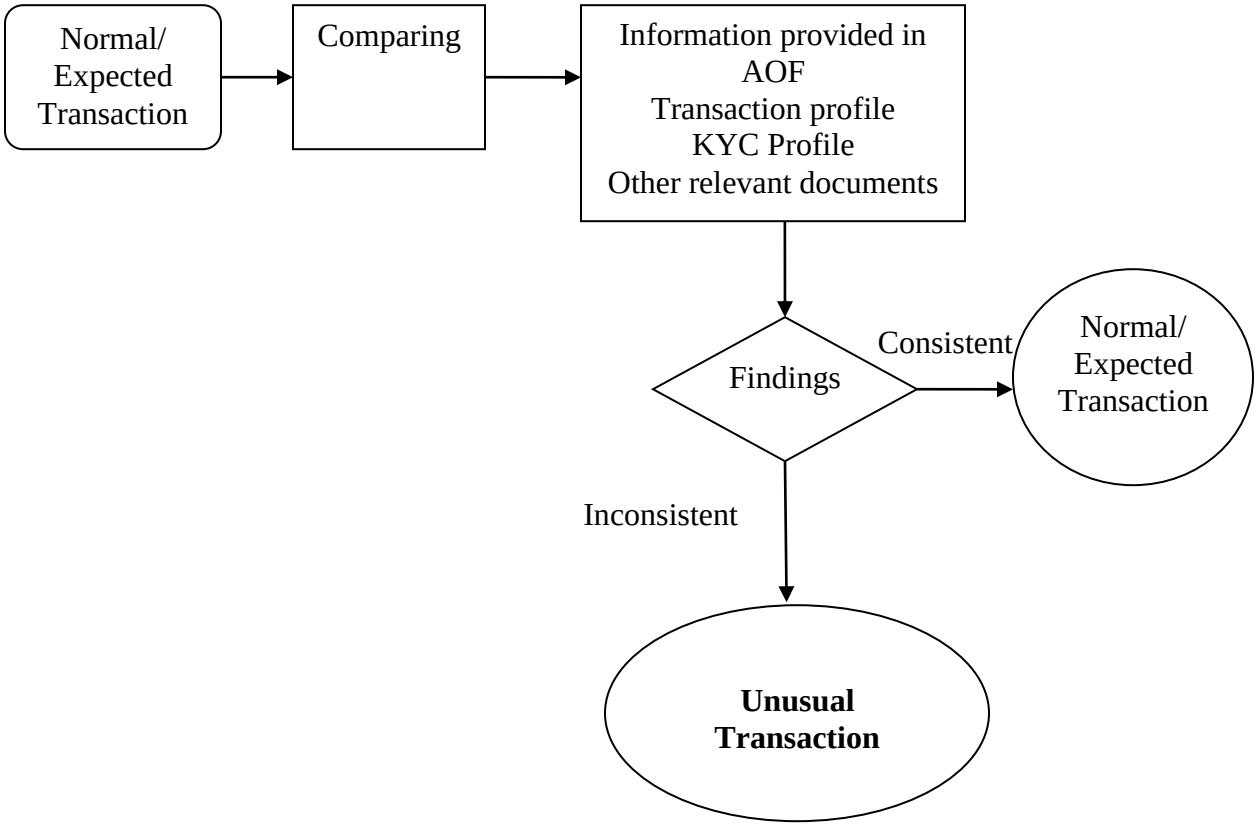
- It is a legal requirement in Bangladesh;
- It helps protect the reputation of FFIL ;
- It helps to protect FFIL from unfounded allegations of assisting criminals, including terrorists;
- It helps the authorities to investigate money laundering, terrorist financing, and other financial crimes.

### 11.3 Identification and evaluation of STR

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

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

- Comparing the KYC profile, if any inconsistency is found and there is no valid reasonable explanation;
- By monitoring customer transactions;
- By using red flag indicator;
- Simply, if any transaction/activity is consistent with the provided information by the customer can be treated as normal and expected. When such transaction/activity is not normal and expected, it may treat as unusual transaction/activity.



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

**Identification**

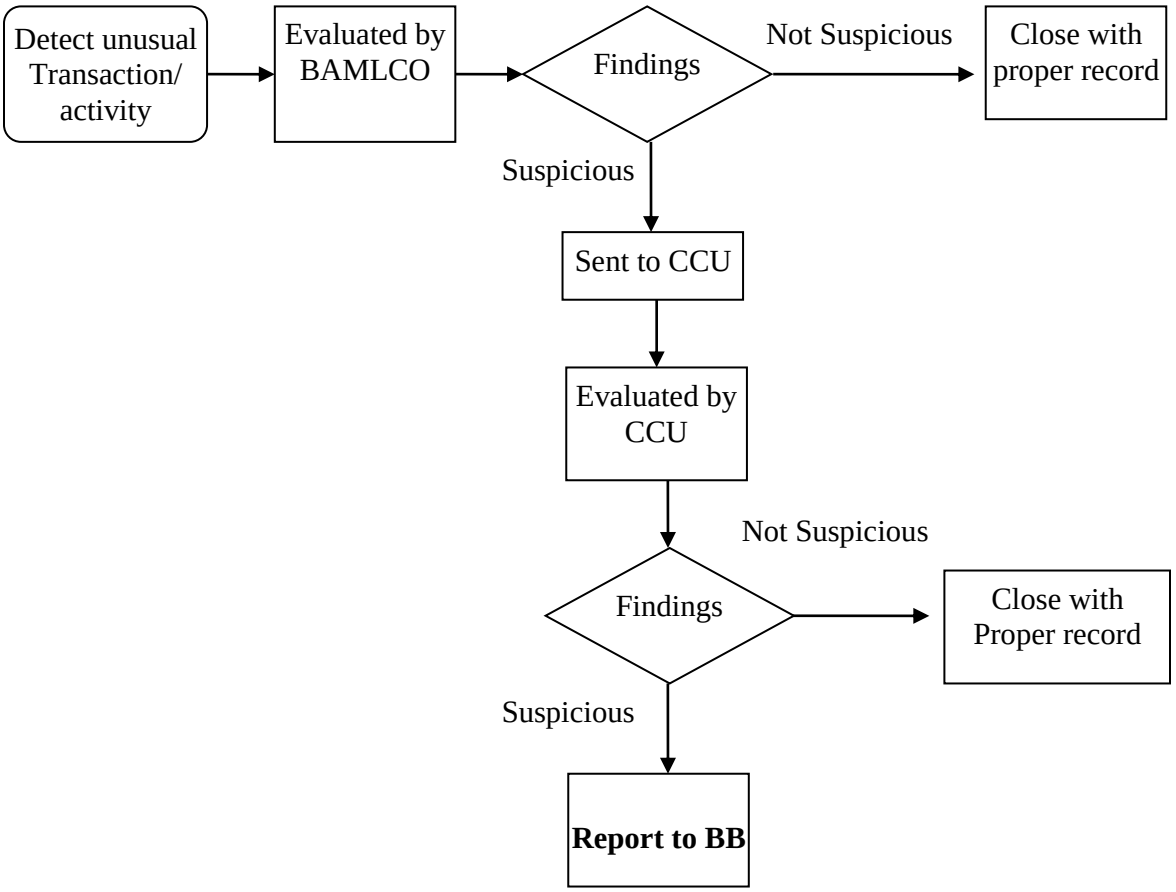
This stage is very vital for STR reporting. Depending on size, need and complexity of financial institutions monitoring of unusual transactions may be automated, manually or both. The use of software can only be complemented managerial oversight and not be replaced the need for constant monitoring of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

**Evaluation**

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

**Disclosure**

This is the final stage and FFIL should submit STR to Bangladesh Financial Intelligence Unit (BFIU) if it is still suspicious. The following flow chart shall shows STR identification and reporting procedures:




**11.4 Risk-based approach**

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

- compare the client's account/transaction history to the client's specific profile information and a relevant peer group, and/or examine the clients account/transaction history against established money-laundering criteria/scenarios, in order to identify patterns of suspicious activity or anomalies;
- establish a process to compare customer or transaction-specific data against risk-scoring models;
- be capable of recognizing patterns and of "learning" which transactions are normal for a client, rather than designating certain transactions as unusual (for example, not all large transaction are unusual and may easily be explained);

- issue alerts if unusual transactions are identified;
- track alerts in order to ensure they are appropriately managed within the institution and that suspicious activity is reported to the authorities as required; and
- maintain an audit trail for inspection by the institution's audit function and by financial institutions supervisors.

### 11.5 Tipping off

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

### 11.6 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.

### 11.7 "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.

### 11.8 Red flags or indicators of STR

FFIL CCU shall consider the following points as red flags or indicators of STR:

#### 11.8.1 Moving customers

A customer 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.

#### 11.8.2 Out of market windfalls

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

business, the distance to its operations may be an attempt to prevent FFIL from verifying there is no business after all. Don't be bullied by FFIL sales personnel who follow the "no question asked" philosophy of taking in new business.

### 11.8.3 Suspicious Customer Behavior

- Customer has an unusual or excessively nervous demeanor.
- Customer discusses FFIL 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.

### 11.8.4 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 FFIL's service area.
- Customer asks many questions about how FFIL 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.

### 11.8.5 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.

### 11.8.6 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.

### 11.8.7 Suspicious employee activity

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

## Section-12: Cash Transaction Report (CTR)

As per the circular of BFIU bearing # 11, FFIL should submit Cash Transaction Report (CTR) in 21st day of every month based on the cash transaction of previous month. FFIL should follow the above rules for reporting CTR:

- If the transaction amount is Tk.10.00 lac or more in each account in a day then it would be included in CTR and report to BFIU through goAML.
- If no transaction is happened in particular month then FFIL should give a certificate through the goAML message board that there is no transaction as CTR.

## Section-13: Conclusion

### 13.1 Governing Law

This Prevention of Money Laundering and Terrorist Financing Manual shall be governed by the existing circulars and guidelines issued by Bangladesh Financial Intelligence Unit (BFIU) and laws and regulations of the Government of the Peoples Republic of Bangladesh.

### 13.2 Approval and commencement

As per the Guidance Notes issued by Bangladesh Financial Intelligence Unit (BFIU) dated September 16, 2012 & master circular issued by BFIU dated June 29, 2015 Fareast Finance & Investment Limited (FFIL) formulated their own Prevention of Money Laundering and Terrorist Financing Manual considering its nature and size of business. This manual is approved by the Board of Directors of Fareast Finance & Investment Limited in the 184th meeting held on April 17, 2018 under agendum # BM201802184-27 and shall be effective from on April 17, 2018.
.

**Appendix-A**

## Know Your Employee (KYE) Form

| | | | |
|---|---|---|---|
| 1. | Name of employee | : | |
| 2. | Father's name | : | |
| 3. | Mother's name | : | |
| 4. | Spouse's name | : | |
| 5. | Present address | : | |
| 6. | Permanent address | : | |
| 7. | Contact number | : | |
| 8. | E-mail ID | : | |
| 9. | Nationality | : | |
| 10. | National ID number | : | |
| 11. | TIN (if any) | : | |
| 12. | Passport number (if any) | : | |
| 13. | Date of birth | : | |
| 14. | Birth registration number | : | |
| 15. | Gender | : | |
| 16. | Blood group | : | |
| 17. | Marital status | : | |
| 18. | Religion | : | |

19. Previous experience:

| **Sl. #** | **Name of organization** | **Position** | **Duration** |
|---|---|---|---|
| | | | |
| | | | |

20. Professional qualification:

| **Sl. #** | **Name of degree** | **Institution** | **Year** |
|---|---|---|---|
| | | | |
| | | | |

21. Academic qualification:

| **Exam Title** | **Concentration/ Major** | **Institute** | **Result** | **Passing Year** |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |

22. Reference(s):

| | | Reference - 1 | Reference – 2 |
|---|---|---|---|
| **Name** | **:** | | |
| **Organization** | **:** | | |
| **Designation** | **:** | | |
| **Address** | **:** | | |
| **Contact #** | **:** | | |
| **E-mail ID** | **:** | | |
| **Relation** | **:** | | |

_____
Signature of the employee
Date:

**For office use only**

Information verified from:

| Sl. # | Name of document | Obtained | |
|---|---|---|---|
| | | Yes | No |
| 1 | One copy color photograph | | |
| 2 | Copy of national ID | | |
| 3 | Copy of TIN (if any) | | |
| 4 | Copy of passport (if any) | | |
| 5 | Copy of birth registration certificate | | |
| 6 | Copy of experience certificate(s) | | |
| 7 | Copy of professional certificate(s) | | |
| 8 | Copy of all educational certificates | | |

Information verified from referee:

| Reference - 1 | Reference – 2 |
|---|---|
| | |

Information regarding present position:

| | | |
|---|---|---|
| Current position | : | |
| Department | : | |
| Duration | : | |

| Description | | Information compiled by | Verified by | Authorized by |
|---|---|---|---|---|
| **Signature** | **:** | | | |
| **Name** | **:** | | | |
| **Designation** | **:** | | | |
| **Remarks** | **:** | | | |

**Appendix-B**

## Suspicious Transaction Report (STR)

| | | | |
|---|---|---|---|
| **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 # | |
| | 2 | Name of the account | |
| | 3 | Nature of account | (Lease/Loan/ML/Factoring/TDR/Other please specify) |
| | 4 | Nature of ownership | (Individual/proprietorship/partnership/company /other, please specify) |
| | 5 | Date of opening | |
| | 6 | Address | |
| **D** | **Account holder details** | | |
| | 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 | Spouse's name | |
| | 10 | Date of birth | |
| | 11 | TIN | |
| | 12 | NID # | |
| | 13 | Passport # | |
| **E** | **Introducer details** | | |
| | 1 | Name of introducer | |
| | 2 | Account # | |
| | 3 | Relation with account holder | |
| | 4 | Address | |
| | 5 | Date of opening | |
| | 6 | Whether introducer is maintaining good relation | |

**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 (please specify)
_____
_____

(Mention summery of suspicious and consequence of events)
[To be filled by the CAMLCO]

**G Suspicious activity information:**
Summery characterization of suspicious activity:

| | | |
|---|---|---|
| a. ☐ Bribery/Gratuity<br>b. ☐ Cheque Fraud<br>c. ☐ Cheque Kitting<br>d. ☐ Commercial Loan Fraud<br>e. ☐ Computer Intrusion<br>f. ☐ Consumer Loan Fraud<br>g. ☐ Counterfeit Check | h. ☐ Counterfeit debit/credit card<br>i. ☐ Counterfeit instrument<br>j. ☐ Credit Card fraud<br>k. ☐ Debit card Fraud<br>l. ☐ Defalcation/Embezzlement<br>m. ☐ False statement<br>n. ☐ Identity Theft | o. ☐ Mortgage Loan Fraud<br>p. ☐ Mysterious Disappearance<br>q. ☐ Misuse of position of self dealing<br>r. ☐ Structuring<br>s. ☐ Terrorist Financing<br>t. ☐ Wire Transfer Fraud<br>u. Other _____ |

**H Transaction details**

| Sl. # | Date | Taka | Type* |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |

*Cash/Transfer/Clearing/TT/etc (add separate paper if necessary)

**I Counter part's details**

| Sl. # | Date | Bank | Branch | Account # | Taka |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

**J Has the suspicious transaction/actively had a material?**
Impact on or otherwise affected the financial soundness: Yes ☐ No ☐

**K Has FFIL taken any action in this context? If yes, give details.**

| |
|---|
| |

**L Documents to be enclosed**

| |
|---|
| 1. Account opening form along with submitted documents;<br>2. KYC profile, Transaction profile;<br>3. Account statement for last one year;<br>4. Supporting voucher/correspondence mention in sl. # H<br>5.<br>6. |

**Signature:**
**(CAMLCO or Authorized officer of CCU)**

Name:
Designation:
Phone #:
Date: