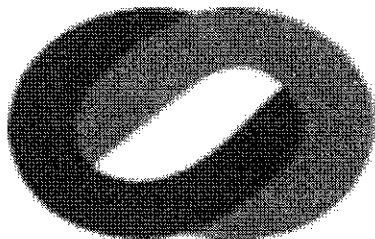


Guidelines on

**Prevention of Money Laundering and
Terrorist Financing**

Of

Strategic Finance & Investments Limited



**STRATEGIC
FINANCE &
INVESTMENTS
LIMITED**



DOCUMENT AUTHORISATION

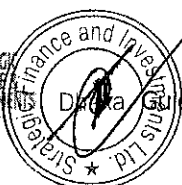
| | |
|-------------------------|---|
| Document Title | Guidelines On Prevention Of Money Laundering And Terrorist Financing |
| Policy Reference | |
| Version | 1.0 |
| Date | January, 2021 |
| Owner | Chief Anti-Money Laundering Compliance Officer |

POLICY DEVELOPMENT HISTORY

| | |
|---|--|
| Author | Mohammad Shajedul Haque Mredha Senior Executive Vice President & CAMLCO |
| Documentation Review | |
| Audit Committee of Strategic Finance & Investments Limited | |
| Approved By | |
| Board of Directors in its 9th Board Meeting held on January 22, 2021. | |



STRATEGIC
FINANCE
INVESTMENTS
LIMITED



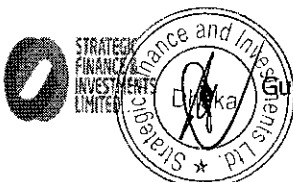


Contents

| | |
|--|----|
| Part-I: Prevention of Money Laundering | 10 |
| Chapter 1 : Introduction | 11 |
| 1.1 Defining Money Laundering and FATF | 11 |
| 1.2 Purpose of money laundering | 13 |
| 1.3 Stages of money laundering | 13 |
| 1.4 Money laundering predicate offenses | 15 |
| 1.5 Reporting organizations | 15 |
| 1.6 Scope and objective of the guidelines | 16 |
| 1.7 How to combat money laundering | 16 |
| Chapter 2 : Vulnerabilities of Strategic Finance & Investments Limited (SFIL) | 17 |
| 2.1 Vulnerabilities of Products and Services | 17 |
| Chapter 3 : Mitigation process-ML/TF risk assessment | 19 |
| 3.1 Introducing risk base approach | 19 |
| 3.2 Assessing risks | 20 |
| 3.3 Risk management and mitigation | 20 |
| 3.4 Risk Management framework | 20 |
| Chapter 4 : Customer Identification and Verification | 22 |
| 4.1 Customer identification | 22 |
| 4.2 Customer profiling | 23 |
| 4.3 Review of KYC profile | 23 |
| 4.4 Taking special care | 23 |
| 4.5 Monitor inconsistent transactions with customer's business/personal profile | 23 |
| 4.6 Preserving customers records | 24 |
| Chapter 5 : Know your customer (KYC), customer due diligence (CDD) and enhanced due diligence (EDD) | 25 |
| 5.1 Benefits of introducing KYC | 25 |
| 5.2 KYC procedures | 25 |
| 5.3 Risk categorization on the basis of KYC | 26 |
| 5.4 Components of KYC | 26 |
| 5.5 Customer acceptance policy | 26 |



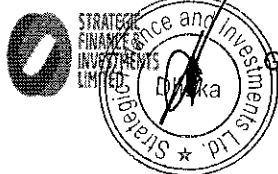
| | | |
|--|---|----|
| 5.6 | Monitoring of high risk accounts and identification of suspicious transactions | 27 |
| 5.7 | What does customer mean | 27 |
| 5.8 | What constitutes a customer's identity | 27 |
| 5.9 | KYC for individual customers | 28 |
| 5.10 | The following points should always bear in mind by responsible officer | 28 |
| 5.11 | KYC for corporate and other entities | 29 |
| 5.12 | KYC for corporate registered abroad | 30 |
| 5.13 | KYC for partnerships and other entities | 30 |
| 5.14 | Powers of attorney/mandates to operate accounts | 30 |
| 5.15 | Transaction monitoring process | 31 |
| 5.16 | What to do if customer due diligence (CDD) will not possible | 31 |
| 5.17 | Politically Exposed Persons (PEPs) and Influential Persons (IPs) | 31 |
| 5.17.1 | Who are Politically Exposed Persons (PEPs) | 32 |
| 5.17.2 | Chief or similar high-ranking positions in an international organization | 32 |
| 5.17.3 | Who should be considered a family member of a PEP? | 33 |
| 5.17.4 | Close associates' of a PEP | 33 |
| 5.18 | What are reporting organizations' obligations under the Regulations? | 33 |
| 5.19 | Ongoing monitoring of accounts and transactions | 35 |
| Chapter 6 : Know your employee (KYE) | | 36 |
| Chapter 7 : Compliance requirement of Strategic Finance & Investments Limited against ML/TF | | 37 |
| 7.1 | Compliance requirement under domestic law | 37 |
| 7.2 | Board approved guidelines for preventing ML and combating TF | 37 |
| 7.3 | Appointment of CAMLCO, DCAMLCO and BAMLCO | 38 |
| 7.4 | Customer identification | 38 |
| 7.5 | Other measures | 38 |
| 7.6 | What to do in case of PEPs and IPs while opening and/or operating account | 39 |
| 7.7 | Appointment and training | 39 |
| 7.7.1 | Employee screening | 39 |
| 7.7.2 | Employee training | 39 |
| 7.8 | Awareness of customers regarding ML/TF | 40 |



| | | |
|---|---|-----------|
| 7.9 | Suspicious transaction report (STR)/suspicious activity report (SAR)..... | 40 |
| 7.10 | Cash transaction report (CTR)..... | 40 |
| 7.11 | Procedure of Self-Assessment Report..... | 40 |
| 7.12 | Independent testing procedures (ITP)..... | 41 |
| 7.13 | Overall assessment report..... | 42 |
| Chapter 8 : Compliance program of Strategic Finance & Investments Limited against ML/TF..... | | 43 |
| 8.1 | Formation of central compliance unit (CCU)..... | 43 |
| 8.2 | Responsibilities of the officials of SFIL..... | 44 |
| 8.3 | The responsibilities of CCU members..... | 45 |
| 8.4 | Appointment of Chief Anti-Money Laundering Compliance Officer (CAMLCO) | 45 |
| 8.5 | Responsibilities of CAMLCO..... | 46 |
| 8.6 | Responsibilities of deputy CAMLCO..... | 47 |
| 8.7 | Responsibilities of BAMLCO..... | 47 |
| 8.8 | Employee training and awareness program..... | 48 |
| 8.8.1 | Employee awareness..... | 48 |
| 8.8.2 | Education and training programs..... | 48 |
| 8.8.3 | Independent audit function..... | 50 |
| 8.8.3.1 | Internal Auditors'..... | 50 |
| 8.8.3.2 | External Auditors'..... | 50 |
| Chapter 9 : Offence of money laundering and punishment..... | | 51 |
| 9.1 | Offence..... | 51 |
| 9.2 | Punishment..... | 51 |
| Chapter 10 : Suspicious Transaction Report/ Suspicious Activity Report (STR/SAR) .. | | 54 |
| 10.1 | General definition..... | 54 |
| 10.2 | Legal definition..... | 54 |
| 10.3 | Obligations of such report..... | 54 |
| 10.4 | Reasons for reporting of STR/SAR..... | 55 |
| 10.5 | Identification and evaluation of STR/SAR..... | 55 |
| 10.5.1 | Identification of STR/SAR..... | 55 |
| a) | Identification:..... | 56 |
| a) | Evaluation:..... | 56 |



| | | |
|--|--|----|
| b) | Disclosure: | 56 |
| 10.6 | Reporting of STR/SAR | 57 |
| 10.7 | Tipping off | 57 |
| 10.8 | Penalties of tipping off | 58 |
| 10.9 | "Safe Harbor" provision for reporting | 58 |
| 10.10 | Indicators of STR/SAR | 58 |
| 10.10.1 | Frequent change of customer address | 58 |
| 10.10.2 | Out of market windfalls | 58 |
| 10.10.3 | Suspicious customer behavior | 58 |
| 10.10.4 | Suspicious customer identification | 59 |
| 10.10.5 | Suspicious non-cash deposits | 59 |
| 10.10.6 | Suspicious activity in credit transactions | 60 |
| 10.10.7 | Suspicious commercial account activity | 60 |
| 10.10.8 | Suspicious employee activity | 60 |
| 10.10.9 | Suspicious activity in an FI setting | 60 |
| Chapter 11 : Reporting cash transaction report (CTR) | | 61 |
| Chapter 12 : Record keeping | | 62 |
| 12.1 | Statutory requirement | 62 |
| 12.2 | Retrieval of records | 63 |
| 12.3 | STR /SAR/CTR and investigation records | 63 |
| 12.4 | Training records | 63 |
| 12.5 | Branch level record keeping | 63 |
| 12.6 | Sharing of record/information | 64 |
| Chapter 13 : Non face to face customer | | 65 |
| 13.1 | Definition | 65 |
| 13.2 | What to do in case of non-face-to-face customer | 65 |
| Chapter 14 : Statement of Compliance | | 66 |
| Chapter 15 : Confidentiality of Information | | 67 |
| 15.1 | Restriction on sharing of record/information as per Money Laundering Prevention (Amendment) Act, 2015 and Anti-Terrorism (Amendment) Act, 2013 | 67 |
| 15.2 | Penalties for disclosing information | 67 |
| Part-II : Combating the Financing of Terrorism | | 68 |



| | | |
|-----|---|----|
| 1. | Introduction | 69 |
| 2. | What is terrorist financing | 69 |
| 3. | International requirement on combating TF and proliferation of weapons of mass destruction | 70 |
| 4. | The link between ML and TF | 70 |
| 5. | Why SFIL must combat financing of terrorism | 70 |
| 6. | Purpose of the policy | 71 |
| 7. | Policy statement | 71 |
| 8. | Enforcement | 71 |
| 9. | Exceptions to the policy | 71 |
| 10. | Procedure | 72 |
| 11. | General procedures for Customer Due Diligence (CDD)/Know Your Customer (KYC) | 72 |
| 12. | Non-profit & NGO sector | 72 |
| 13. | Training and awareness of the employees | 73 |
| 14. | Self-assessment | 73 |
| 15. | Independent testing procedures | 73 |
| 16. | Monitoring | 73 |
| 17. | Responsibilities | 74 |
| 18. | Customer acceptance policy | 75 |
| 19. | Penalties for non-compliance of Anti-Terrorism (Amendment) Act, 2013 | 75 |
| 20. | Schedule of Anti-Terrorism (Amendment) Act, 2013 | 76 |
| | "Annexure-A" | 79 |
| | "Annexure-B" | 80 |
| | "Annexure-C" | 82 |
| | "Annexure-D" | 83 |
| | "Annexure-E" | 84 |
| | "Annexure-F" | 86 |
| | "Annexure-G" | 89 |
| | "Annexure-H" | 93 |
| | "Annexure-I" | 97 |



PREFACE

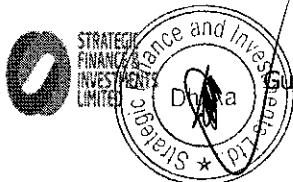
Money Laundering is a serious threat to financial system of all countries and it leads to destruction of the country's financial market, payment mechanism, and infrastructure and endanger the country's sovereignty as a whole. Nowadays Money Laundering and Terrorist financing has emerged as the alarming financial crime in the global economy. To combat with these, Government of Bangladesh has enacted the "Money Laundering Prevention Act 2012 (as amended in 2015)" and "Anti-Terrorism Act 2009 (as amended in 2013)". Besides, Bangladesh Bank vides DFIM circular #7 dated 4 October, 2012 has declared 'Money laundering and Terrorist Financing Risk' as one of the core risks of the financial institutions. In this regard, Bangladesh Financial Intelligence Unit (BFIU) has also issued 'Guidance Note on prevention of money laundering and terrorist financing'. In this context, Strategic Finance & Investments Limited (referred as "SFIL") prepares its own policy named hereafter "Guidelines on Prevention of Money Laundering and Terrorist Financing".

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

To ensure compliance with these enactments, Strategic Finance & Investments Limited established a Central Compliance Unit (CCU) (Sec: 8.1) under the leadership of CAMLCO who is not lower than the third rank in seniority in organizational hierarchy. Besides, SFIL has designated one high level officer as Deputy Chief Anti- Money Laundering Compliance Officer (Deputy CAMLCO) in the CCU and Branch Anti-Money Laundering Compliance Officer (BAMLCO) in the branch level. The CAMLCO is the Head of CCU and has vast working experience which is more than required.

Compliance requirements of the above enactments which Strategic Finance & Investments Limited or its employees should always bear in mind are as follows:

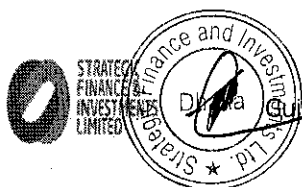
1. Report to BFIU proactively and immediately, facts on suspicious, unusual or doubtful transactions (STR/SAR) likely to be related to money laundering. [Ref: Guidance Notes on STR/SAR by BFIU and 25(1) (d) of MLPA 2012].
2. Maintain confidentiality while sharing customer's account related information. [Ref: MLPA 2012 (as amended in 2015) and ATA 2009 (as amended in 2013)].
3. Reporting Organizations shall consider the confidentiality of the reporting of STR/SAR. [Ref: Guidance Notes on STR/SAR by BFIU and Sec 6 of MLPA 2012, BFIU Master Circular#12 dated June 29, 2015 and FATF Recommendation #21].
4. Not to open or maintain numbered or anonymous account.
5. Know your employee (KYE) and know your customer (KYC).
6. PEPs (as well as their family members and persons known to be close associates) are required to be subject to undertake enhanced due diligence by a reporting organization. [Ref: Guidance Notes on PEPs by BFIU and ML circular # 14 dated 25 September 2007].
7. Customer Due Diligence (Chapter-5) should be exercised in the case of customer identification, acceptance, monitoring and reporting of suspicious transactions.



8. Self-assessment of the effectiveness of the AML/CFT program should be carried on half yearly basis by the BAMLCO and the results of the same to be communicated to the ICC and CCU. [Ref: BFIU Master Circular#12 dated June 29, 2015].
9. The ICC shall carry out independent testing procedure (ITP) to check the adequacy of AML/CFT policies and conduct audit in case of major non-compliance, if any, and report to CCU for taking necessary action;. [Ref: BFIU Master Circular#12 dated June 29, 2015].
10. Preserve, at least for 5 (five) years, all necessary records on transactions, to comply with information requests from the competent authorities like BFIU and other legal authorities. However in compliance with the provision of the Companies Act, 1994 (under subsection 5 of section 181) the same may be retained up to 12 (twelve) years [Ref: BFIU Master Circular#12 and U/s 25(1) of MLPA 2012] and
11. Shall be fully complied with BFIU Master Circular#12, dated: June 29, 2015 issued and to be issued by BFIU and other prevailing and or future laws and regulations relating to AML/CFT.

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

In case of any conflict between this AML/CFT policy and the Money Laundering Prevention (Amendment) Act, 2015 and Anti-Terrorism (Amendment) Act, 2013, the Original Act, Regulations; and Circulars, Directive etc. of BFIU shall prevail.



Part-I: Prevention of Money Laundering



Chapter 1 : Introduction

Money laundering is the generic term used to describe the process by which criminals try to disguise the original ownership and control of the proceeds of criminal conduct by making them appear legal. The processes by which criminally derived property may be laundered are extensive. Though criminal money may be successfully laundered without the assistance of the financial sector, the reality is that hundreds of billions of dollars of criminally derived money is laundered through various sectors, every year. The nature of the services and products offered by the financial services industry carries the inherent risk of being abused by money launderers.

The act of laundering is committed in circumstances where a person is engaged in an arrangement of providing a service or product and that arrangement involves the proceeds of crime. These arrangements include a wide variety of business relationships e.g. banking, fiduciary and investment management.

The requisite degree of knowledge or suspicion will depend upon the specific offence but will usually be present where the person providing the arrangement, service or product; knows, suspects or has reasonable grounds to suspect that the property involved in the arrangement represents the proceeds of crime. In some cases the offence may also be committed where a person knows or suspects that the person with whom he or she is dealing is engaged in or has benefited from criminal conduct.

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.

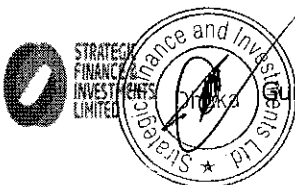
Money laundering has a major impact on a country's economy as a whole, impeding the social, economic, political, and cultural development of societies worldwide. Both money laundering and terrorist financing can weaken individual financial institution, and they are also a threat to a country's overall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

The process of money laundering and terrorist financing (ML/TF) is very cumbersome. The money launderers always try to invent more and more complicated and sophisticated procedures by using newer technology for money laundering. To address these challenges, the global community has taken various initiatives against ML/TF.

1.1 Defining Money Laundering and FATF

International perspective

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



- The conversion or transfer of property, knowing that such property is derived from any [drug trafficking] offense or offenses or from an act of participation in such offense or offenses, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an offense or offenses to evade the legal consequences of his actions;
- The concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property, knowing that such property is derived from an offense or offenses or from an act of participation in such an offense or offenses, and;
- The acquisition, possession or use of property, knowing at the time of receipt that such property was derived from an offense or offenses or from an act of participation in such offense or offenses.

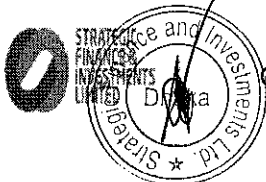
FATF definition

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

National legal framework

Section 2 (v) of the Money Laundering Prevention (Amendment) Act, 2015 defined ML as follows:

- i. Knowingly moving, converting, or transferring proceeds of crime or property involved in an offence for the following purposes:-
 - a. Concealing or disguising the illicit nature, source, location, ownership or control of the proceeds of crime; or
 - b. 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.

1.2 Purpose of money laundering

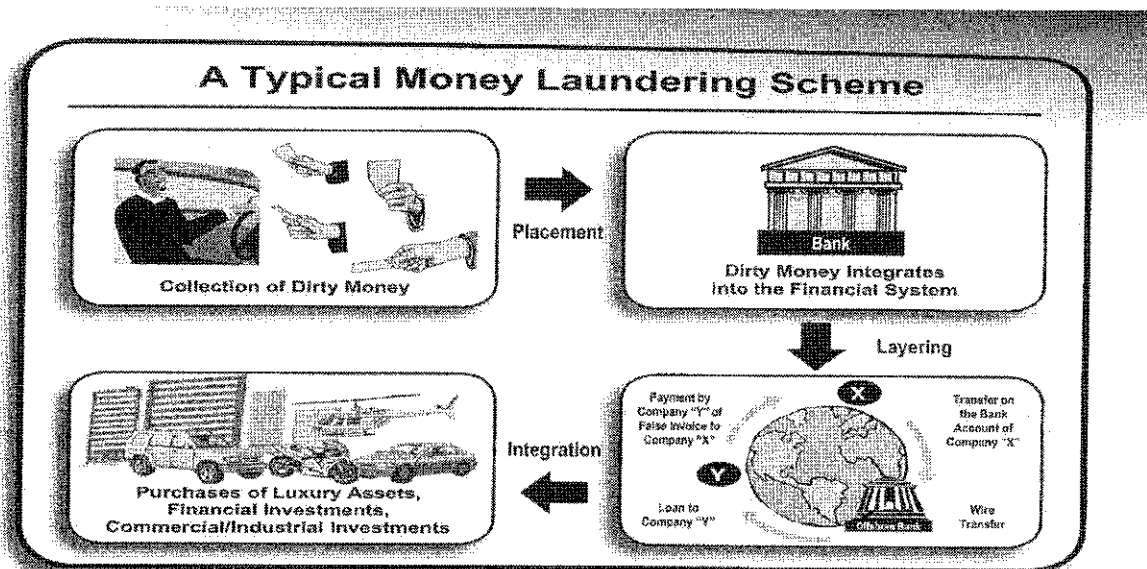
The purpose of money laundering is to cease the connections between the money and the crime from which ill money has been generated. In other words, money laundering disguises or conceals the illicit origin of money generated through criminal activities.

Launderers engaged themselves in money laundering for 4 (four) main reasons:

- i. To organize and run criminal activity using financial channel to get financial benefit;
- ii. To conceal or disguise the source of their wealth to avoid prosecution;
- iii. To cover ill-gotten gains from suspicion and protect them from forfeiture; and
- iv. To conceal their existence or alternatively, give them a legitimate look.

1.3 Stages of money laundering

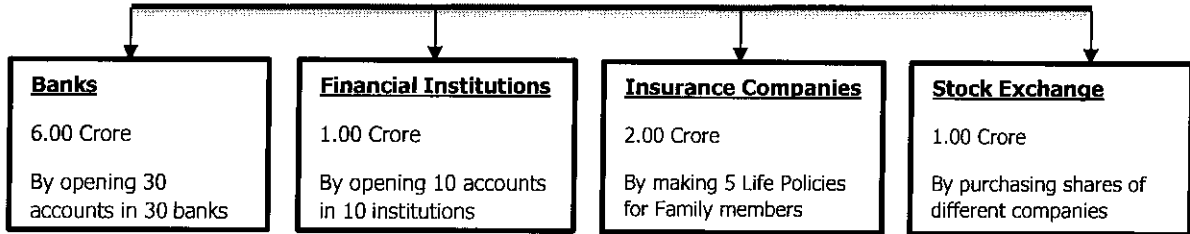
Money laundering is not a single act but a process accomplished in 3 basic stages placement, layering and integration which may comprise numerous transactions by the launderers. A typical money laundering scheme is illustrated below:



Source: United Nations Office on Drugs and Crime

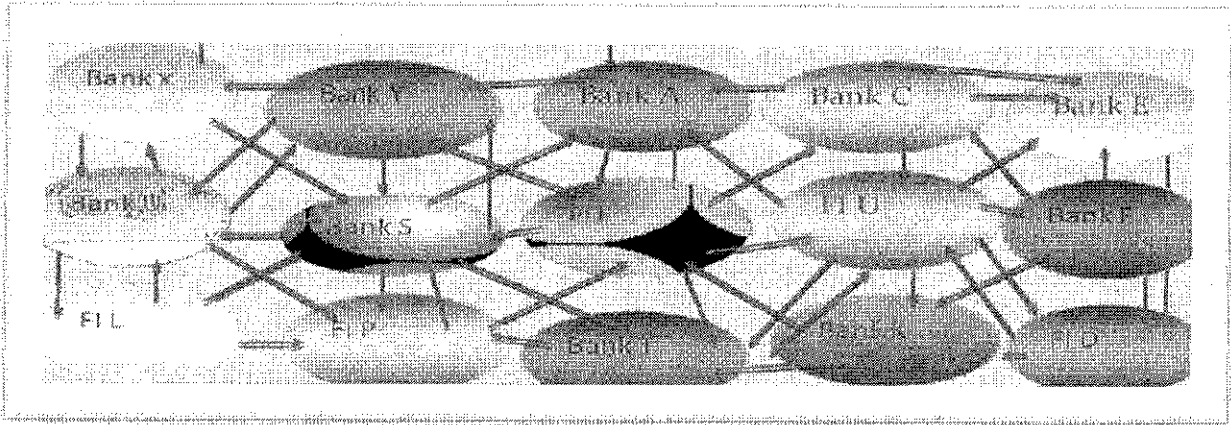
Placement means the initial deposit of illegally derived funds either through its introduction into the financial system; through the purchase of high value goods; or by physical cross-border transportation.

PLACEMENT: EXAMPLE



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

LAYERING: EXAMPLE

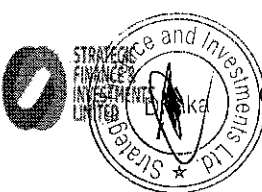
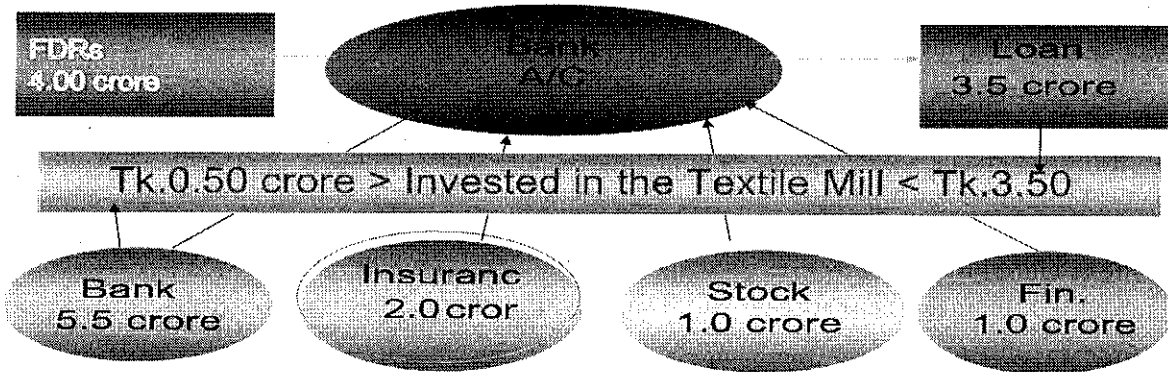


Mr. X moved money deposited in the banks through a series of economically meaningless transactions

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

INTEGRATION: EXAMPLE

Mr. X formed a company namely M/S Shah Ali Textile Ltd and opened an A/C in ABC Bank



1.4 Money laundering predicate offenses

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

- a) Corruption and bribery;
- b) Counterfeiting currency;
- c) Counterfeiting deeds and documents;
- d) Extortion;
- e) Fraud and forgery;
- f) Illegal trade of firearms;
- g) Illegal trade in narcotic drugs, psychotropic substances and substances causing intoxication;
- h) Illegal trade in stolen and other goods;
- i) Kidnapping, illegal restraint and hostage taking;
- j) Murder, grievous physical injury;
- k) Trafficking of woman and children;
- l) Black marketing;
- m) Smuggling of domestic and foreign currency;
- n) Theft or robbery or dacoit or piracy or hijacking of aircraft;
- o) Unauthorized cross-border transfer of domestic and foreign currency;
- p) Dowry;
- q) Smuggling and offences related to customs and excise duties;
- r) Tax related offences;
- s) Infringement of intellectual property rights;
- t) Terrorism or financing in terrorist activity;
- u) Adulteration or the manufacture of goods through infringement of title;
- v) Offences relating to the environment;
- w) Sexual exploitation;
- x) Insider trading and market manipulation using price sensitive information relating to the Capital market in share transactions before it is published for general information to take Advantage of the market and attempting to manipulate the market for personal or institutional gain;
- y) Racketeering; and
- z) Any other offence declared as predicate offence by Bangladesh Financial Intelligence Unit (BFIU) with the approval of the Government, by notification in the Official Gazette, for the purpose of this Act.

1.5 Reporting organizations

- a) Banks;
- b) Financial Institutions;
- c) Insurer;
- d) Money changer;
- e) Any company or institution which remits or transfers money or money value;
- f) Any other Institution carrying out its business with the approval of Bangladesh Financial Intelligence Unit (BFIU);
- g) Stock dealer and stock broker;
- h) Portfolio manager and merchant banker;
- i) Securities custodian;
- j) Asset Manager;
- k) Non-profit organization;



- l) Non-government organization;
- m) Cooperative society;
- n) Real estate developer;
- o) Dealer in precious metals or stones;
- p) Trust and company service provider;
- q) Lawyer, notary, other legal professional and accountant; and
- r) Any other institution which BFIU may, from time to time, notify with the approval of the Government.

1.6 Scope and objective of the guidelines

This policy is applicable for all sorts of transactions, products, operations and other relevant activities of SFIL including branch/es. The Company would ensure compliance with this AML/CFT Guidelines or as prescribed by law and/or the Bangladesh Financial Intelligence Unit (BFIU) circulars, directives etc. issued from time to time whichever more exhaustive.

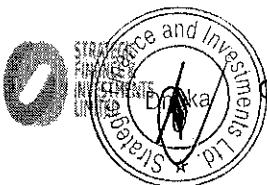
The objective of this policy is to ensure that SFIL has designed and implemented processes and procedures that are consistent with regulatory guidelines and the goals and purposes of the AML/CFT Act.

The overall framework for AML/CFT regime designed in SFIL so that the business units and other concerned will take responsibility for:

- a) Verifying true identity of customers prior to provide any service;
- b) Reporting all STR/SAR/CTR to Bangladesh Financial Intelligence Unit (BFIU);
- c) Keeping appropriate records at least for 5(five) years as determined by BFIU;
- d) Providing, from time to time, information as required by BFIU and other regulatory authorities; and
- e) Developing, implementing and complying with all AML/CFT related legal requirements.

1.7 How to combat money laundering

Money laundering potentially devastates the economy, social security and safety. ML is a process of making crime worthwhile. It provides fuel for drug dealers, smugglers, terrorists, illegal arms dealers, corrupt public officials, and others to operate and expand their criminal initiatives. ML diminishes government tax revenue and therefore, indirectly harms honest taxpayers. It also makes government tax collection more difficult. In order to preventing ML, SFIL should always pay particular attention to the fundamental principle of good business practice i.e. Customer Due Diligence (CDD), Enhanced Due Diligence (EDD), Know Your Customer (KYC) and Know Your Employee (KYE). Having a sound knowledge of a customer's business and pattern of financial transactions and commitments-are the best methods by which SFIL and its officials will try to recognize and protect ML/TF.



Chapter 2 : Vulnerabilities of Strategic Finance & Investments Limited (SFIL)

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

2.1 Vulnerabilities of Products and Services

➤ Lease/Term Loan Finance

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

➤ Factoring

SFIL introduced its Factoring financing recently considering its different market segment. Using its complex business mechanism, the supplier and the buyer may ally together to legalize their proceeds of crime. Without conducting any bona fide transaction, the supplier may get finance from SFIL and SFIL may get repayment from buyer. SFIL 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.

➤ Personal Loan/Car Loan/Home Loan

Any person can take personal loan from SFIL 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.

➤ SME/Women Entrepreneur Loan

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

➤ Deposit Scheme

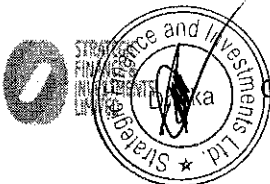
SFIL sell deposit products with at least a three months maturity period. The depositor may en-cash



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

➤ **Loan Backed Money Laundering**

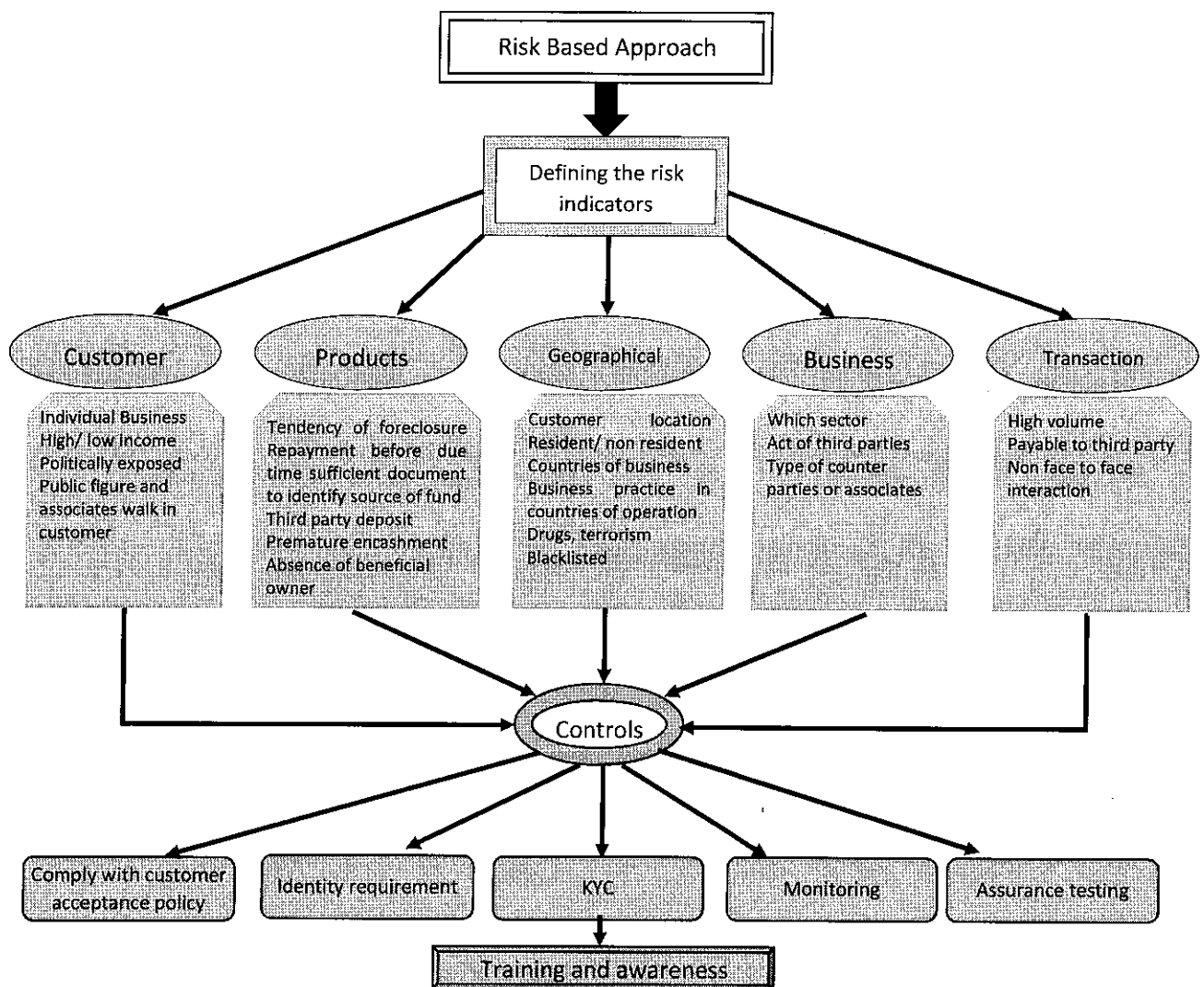
In the "loan backed" money laundering method, a criminal provides an associate with a specific amount of illegitimate money. The associate then provides a "loan or mortgage" back to the money laundering for the same amount with all the necessary "loan or mortgage" documentation. This creates an illusion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



Chapter 3 : Mitigation process-ML/TF risk assessment

3.1 Introducing risk base approach

The risk-based approach is an essential component of the effective implementation of the FATF Recommendations. Government, competent authorities, financial institutions, designated non-financial business and professions (DNFBPs) and other reporting entities are sole responsible to understand, identify, assess, and take effective action to mitigate ML/TF risks. A Risk Based control process should be as follows:



An integrated risk-based system depends mainly on a proper assessment of the relevant risk sectors, products, services, and customers 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. In pursuance



of the Wolfsburg Group guidelines, a risk-based monitoring system of SFIL should:

- Compare the customer's account/transaction history to the customer's specific profile information and a relevant peer group, and/or examine the customer's account/transaction history against established ML 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 customer, 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.

These will help in design and implementation of this approach for mitigating ML/TF risks.

3.2 Assessing risks

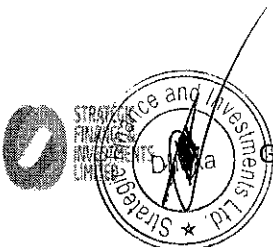
SFIL should be required to take appropriate steps to identify and assess ML/TF risk arisen from or through customers, products or services and transactions or delivery channels and geographical presence. SFIL should document assessment result in order to be able to demonstrate their basis, keep assessment result up-to-date and provide assessment result to the competent authority.

3.3 Risk management and mitigation

Risk management is a systematic process of recognizing risk and developing both minimize and manage the risk. To mitigate the vulnerabilities of ML/TF risks, SFIL should require to establish policies, controls and procedures that enable to manage and mitigate the risks that have been identified in assessment process. SFIL also requires to monitor the implementation of those controls and to enforce more stringent policy, if necessary. The mitigation policies, controls and procedures must be approved by senior management.

3.4 Risk Management framework

A risk management framework consists of establishing the internal and external context within which the designated service is to be provided, risk identification, risk assessment or evaluation and risk treatment-mitigating, managing, control, monitoring and periodic reviews. A risk management framework is briefly stated in a tabular form as follows:



| | |
|---|---|
| Stage-1: Risk identification | |
| Identification of main ML/TF risks | Customer |
| | Product |
| | Sector |
| | Delivery Method |
| | Country/Jurisdiction |
| Identification of regulatory risks | Failure to report STR/SAR/CTR |
| | Inappropriate customer verification |
| | Inappropriate record keeping |
| | Lack of AML/CFT program |
| Stage-2: Risk assessment | |
| Measure the size and importance of the risk | Likelihood-Chance of the risk happening Impact- |
| | The amount of loss or damage on risk Likelihood |
| | X Impact-Level of risk (risk score) |
| Stage-3: Risk treatment | |
| Manage business risk | Minimize and manage risks |
| | Apply strategies, policies and procedures |
| Manage regulatory risk | Put in place system and controls |
| | Carry out risk plan and AML/CFT program |
| Stage-4: Risk monitoring and review | |
| Monitor and review risk plan | Develop and carry out monitoring process |
| | Keep necessary records |
| | Review risk plan and AML/CFT program |
| | Execution internal audit or assessment |
| | Preparation AML/CFT compliance report |

Bangladesh Financial Intelligence Unit (BFIU) issued a Circular Letter No. 04: dated July 30, 2015 on Money Laundering and Terrorist Financing Risk Assessment Guidelines for Financial Institutions. The guidelines can be found in the following link for more understanding:

https://www.bb.org.bd/bfiu/bfiu_lawguidelist.php



Chapter 4 : Customer Identification and Verification

A meaningful anti-money laundering compliance program should include identification and verification of customers at the stage of opening account or establishing financial transaction or relationship. Accordingly, the Company should ensure to:

- i. Verify the identity of any person/individual concern/company (hereinafter called as "customer") while pursuing to open an account to the extent reasonable and practicable;
- ii. Maintain records of the information used to verify a customer's identity, including name, address and other identifying information; and
- iii. Verify the UNSCR list (1267/1999 and 1373/2001), banned list of Bangladesh Government of known or suspected terrorists or terrorist organizations or other national or international sanction lists using SFIL's own software to determine whether a person pursuing to open an account appears on any such lists.

The following options are recommended for concerned officers of Head Office as well a branch/es to consider in developing customer identification process:

4.1 Customer Identification

SFIL should not keep anonymous or accounts in fictitious name/s. Company should undertake customer due diligence measures, including identifying and verifying the identity of their customers when:

- i. Establishing business relations;
- ii. Carrying out occasional transactions;
- iii. There is a suspicion of money laundering or terrorist financing; and
- iv. The financial institution has doubts about the reliability or adequacy of previously obtained customer identification data.

In order to fulfill identification requirements SFIL should, where necessary, take measures to:

- i. Verify the legal existence and structure of the entity by obtaining either from a public register or from the customer or both, proof of incorporation, including information concerning the customer's name, legal form, address, directors and provisions regulating the power to bind the entity, as the case may be;
- ii. Verify that any person purporting to act on behalf of the customer is so authorized and identify that person;
- iii. No account should be opened without satisfactory identification, and proper introduction, where applicable. In fact before opening an account concerned officer should interview the customer to assess his need for opening an account, his business, engagement etc.;
- iv. Customer's residence (permanent and present) or place of business to be carefully considered. If it is not in the area where SFIL or branch serves, in that case opening an account at that location may need to be justified;
- v. Should issue thanking letters to the customers for opening account or establishing business



relations towards verification of address (attached as "Annexure-A"); and

- vi. The source of funds used to open the account shall be known and commensurate with the account opener's details.

4.2 Customer profiling

- a) Obtaining and documenting the customer's basic background and information;
- b) Use those information to evaluate the appropriateness and reasonableness of the customer's transaction activity;
- c) The customer's expected transaction trends;
- d) Net income; and
- e) Determine the source of the customer's funds.

4.3 Review of KYC profile

KYC shall be reviewed on a regular interval i.e. in case of high risk customer at least once in a year and in case of low risk customer once in every two years for:

- i. Monitoring transactions and activities; or
- ii. Renewal of an account; or
- iii. Customer visited SFIL; or
- iv. Any change in introductory information of customer;
- v. Periodic discussions with the customer relating to their business activities or future plan of the business; or
- vi. Any other activities as deemed necessary.

4.4 Taking special care

Responsible officer of business department should monitor customer's borrowing profile in the course of business to ascertain repayments or settlement of loan or loan drawdown is in line with the customer business activities. They shall also take special care on the following cases:

- i. On high risk customer;
- ii. In case of deposit of significant amount which inconsistent with customer profile; and
- iii. Deposit of funds into company's accounts, usually in amounts below the threshold limit set by Bangladesh Financial Intelligence Unit (BFIU).

4.5 Monitor inconsistent transactions with customer's business/personal profile

Responsible officer shall closely monitor the customer's account in case:

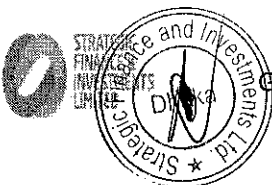
- i. Where they make payments in cash rather than using banking channel;
- ii. Operate retail business but made substantial payments against loan which indicates that the customer may have another undisclosed source of income; and



- iii. Deposit of large volume of cash which does not match with the customer's business profile.

4.6 Preserving customers records

SFIL should preserve all necessary records of transactions as per Bangladesh Financial Intelligence Unit (BFIU) circular in force, to enable them to supply information as desired by the competent authorities. Such records must be sufficient to permit construction of individual transactions so as to provide, if necessary, evidence for prosecution for criminal behavior. They also should keep records on customer identification e.g. copies or records of official identification documents like NID, passport copy, identity card, driving license or any other documents acceptable to the Company, account files and business correspondence for a minimum of 5 (five) years even after the account is closed as advised BFIU. These documents should be available to domestic competent authorities in the context of relevant criminal prosecutions and investigations.



Chapter 5 : Know your customer (KYC), customer due diligence (CDD) and enhanced due diligence (EDD)

Generally, Know Your Customer (KYC) policy is implemented to confirm a customer's identification program. The term is also used to refer to the regulation which governs these activities. KYC is mostly used in financial institutions and other reporting authorities as defined by the regulators. They use KYC to identify customers and ascertain relevant information in doing business/relationship with them. In wider terms, KYC processes are also employed by companies of all sizes for the purpose of ensuring AML/CFT compliances. KYC policies are becoming much more important globally to protect financial fraud, money laundering, terrorist financing etc.

Generally SFIL should never establish a relationship with a customer until it knows the customer's true identity. If a potential customer is unwilling to provide necessary information and documents, the relationship should not be established.

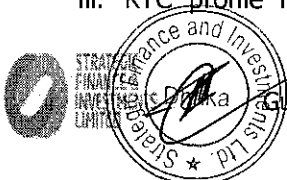
5.1 Benefits of introducing KYC

KYC-

- i. helps detect suspicious activity in a timely manner;
- ii. promotes compliance with all relevant laws;
- iii. promotes safe and sound financial transactions and best business practices;
- iv. minimizes the risk that the Company may encounter for illicit activities;
- v. reduces the risk of government seizure and forfeiture of a customer's loan collateral when they are involved in criminal activities or ML/TF issues, and
- vi. Protects Company's reputational risk.

5.2 KYC procedures

- i. Before opening an account, due diligence is required to be performed on all prospective customers. This process should be completed by fulfilling the documentation requirements (duly filled in application form, references, source of funds, applicable identities etc.) with a Know Your Customer (KYC) profile which is used to record a customer's source of fund, expected transaction activity at its most basic level.
- ii. Once the identification procedures are completed and relationship with the customer is established, SFIL should monitor behavior of customers to ensure that it is consistent with the nature of business as was stated while establishing relationship/opened account. Concerned officer will be responsible for reporting suspicious transactions undertaken by the customer, review & updating customer's KYC profile for any significant changes in their lifestyle (e.g., change of employment status, increase in net worth etc.) and by monitoring the transaction activity over the customer's account on a periodic basis.
- iii. KYC profile must contain the basic information about the customer like name, address,



tel/cell/fax numbers, e-mail address, and line of business, annual sales and other relevant information. If the customer is a PEPs/IPs, the account is to be taken special care and requisite EDD should be done.

- iv. The KYC profile information will also include the observations of the concerned officer of Head Office or branch/es regarding business premises (whether rented or owned), type of customer's business, method of transaction preferred by the customer (whether in cheque or cash). The concerned officer will record those observations and put signature on the KYC form.
- v. The KYC profile leads to risk classification of the accounts as high/low risk.

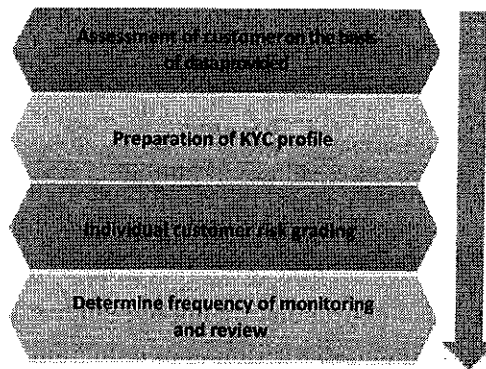


Figure: KYC Flowchart

5.3 Risk categorization on the basis of KYC

While opening accounts, the concerned officer must assess the inherent risks that the accounts might carry relating to "Money Laundering", and must classify the accounts as either 'High Risk' or 'Low Risk'. The risk assessment may be made using the Risk Grading Matrix given at "**Annexure-C**" by which risk shall be categorized using numeric scale to denote risks.

5.4 Components of KYC

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

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

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

5.5 Customer acceptance policy

Selection of customer is an important factor for Banks and NBFIs. SFIL takes into consideration of all the relevant factors in case of opening/operating customer's accounts such as customer's background, business/personal activities, business risks, credit worthiness, political influence, social status, other



basic information and other risk factors.

On the other hand, to prevent of ML/TF risks KYC, CDD, EDD, KYE are the important tools. Lack of precaution in the above mentioned factors might result in serious customer and counterparty risks, especially reputation, operational, legal and compliance risks. Collection of sufficient information about the customer is the most effective defense for combating ML/TF activities. As per Money Laundering Prevention (Amendment) Act, 2015 each FI is required to keep satisfactory record of the customers. On the other hand, each FI is also required to make necessary arrangement to prevent transactions related to crimes as described in Anti-Terrorism (Amendment) Act, 2013. It also requires identifying, under these laws, suspicious transactions/activity with due care and diligence. Pursuant to the above legal bindings, Guidance Notes issued by Bangladesh Financial Intelligence Unit (BFIU) on AML/CFT and global standards, SFIL has developed a Customer Acceptance Policy as stated at "Annexure-B".

5.6 Monitoring of high risk accounts and identification of suspicious transactions

High value single transaction conducted in a single DD, PO, TT and Electronic Transfer by any person or institution involved in a financial transaction may pose reputational and other risks to SFIL. In this case if a transaction appears abnormal in relation to the usual transaction of the concerned person or institution that transaction will be treated as high value and suspicious transaction.

5.7 What does customer mean

As per Section – 2(j) of Money Laundering Prevention (Amendment) Act, 2015:

"Customer" means any person or persons or entity or entities that may be defined by Bangladesh Financial Intelligence Unit (BFIU) from time to time.

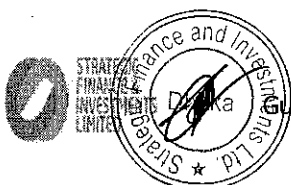
For the purpose of KYC procedure a "Customer" means as per BFIU Master Circular#12, dated June 29, 2015:

- i. Any person or institution maintaining an account of any type with SFIL;
- ii. The person or institution as true beneficial owner in whose favor the account is operated; and
- iii. The trustee, intermediary or true beneficial owner of the transaction of the accounts operated by the trust and professional intermediaries (such as lawyer/law firm, chartered accountant, etc.) under the existing legal infrastructure.

5.8 What constitutes a customer's identity

Identity generally means a set of attributes which uniquely defines a natural or legal person. There are two main constituents of a person's identity out of a range of legal persons (an individual, corporate body, partnership, etc.). For the purposes of this guidance, the two constituents are:

- i. The physical identity (e.g. birth certificate, TIN/VAT registration, passport/NID, driving license etc.); and



- ii. The activity undertaken.

Confirmation of a person's address is also useful in determining whether a customer is resident in a high-risk country. Information of both residential and nationality status of a customer are also necessary tools of identity. It needs 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.

5.9 KYC for individual customers

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

- i. Correct name and/or names used;
- ii. Parent's names;
- iii. Date of birth;
- iv. Current and permanent address;
- v. Details of occupation/employment and sources of wealth or income; and
- vi. Contact information, such as – mobile/telephone number etc.

5.10 The following points should always bear in mind by responsible officer

The following points should always be borne in mind by a responsible officer while opening an account or making financial transaction with any prospective customer:

- i. SFIL shall not allow any non-face to face contact;
- ii. Particular care should be taken in accepting documents/identities which are easily be made false or duplicate;
- iii. In respect of joint accounts where the surname and/or address of the account holders differ,
- iv. The name and address of all account holders should be verified;
- v. Any subsequent change of the customer's name, address, or employment details of which the SFIL becomes aware should be recorded as part of the KYC process for review customer's profile;
- vi. All documents collected for establishing relationship must be filled in with supporting evidences;
- vii. Details of the introducer 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;
- viii. In the case of socially or financially disadvantaged people such as the elderly, the disabled,



students and minors, the identity of these persons can be verified from an original or certified copy of alternative document, preferably one with a photograph. Certificate or confirmation from lawyer, accountant, director or manager of a regulatory or regulated institution, a notary public, a member of the judiciary or a senior civil servant may be acceptable to SFIL in this behalf. The Certifier must sign on the copied document and clearly indicate his position or capacity on it with a contact address and phone number;

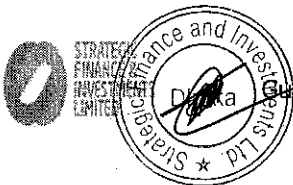
- ix. The normal identification procedures set out above should be followed. Moreover, in case of minor parents/legal guardians KYC procedure must be followed;
- x. Documents of identity which do not bear photographs or signatures are not acceptable. More importantly, checking of authenticity of the documents is a must;
- xi. To verify the customer's permanent and present address passport/NID and recent utility bill's copy can be checked; and last but not least;
- xii. The original copy of (i) current valid passport; (ii) valid driving license; (iii) NID; (iv) employer provided ID card, bearing the photograph and signature of the applicant should be used to verify identify the customer and certified copies of the same should be procured and preserved for record.

5.11 KYC for corporate and other entities

The principal requirement for the corporate bodies is to verify its legal existence and find out person behind the entity to identify who are controlling business and the company's assets, with particular attention being paid to any shareholders or others who exercise a significant influence over the day to day affairs of the company. Enquiries should be made to confirm that the company exists for a legitimate trading or economic purpose.

The following documents should be obtained from companies;

- i. Certificate of incorporation or duly certified by RJSC, address of the registered office, and place of business;
- ii. Certified copy of Memorandum and Articles of Association, or by-laws of the customer;
- iii. Copy of the board resolution to open account/maintain relationship with delegation of authority/ies to operate accounts;
- iv. Explanation of the nature of the applicant's business, the source of funds, and a copy of the last available financial statements, where applicable;
- v. Satisfactory evidence of the identity of each of the principal beneficial owners being any person holding 20.00% interest or more or with principal control over the company's assets and any person/s 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;
- vi. 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;

- vii. Copies of the Schedule X and Form XII; and
- viii. Any other relevant documents require establishing relationship/financial transaction.

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 for the above case:

- i. All of the directors who will be responsible for operation of the account;
- ii. All the authorized signatories for the account/transaction;
- iii. All the holders of powers of attorney to operate the account/transaction;
- iv. The beneficial owner(s) of the company, where applicable; etc.

Where the institution already knows their identities and identification records comply with the requirements of these notes, there is no need to verify identity again. When authorized signatories change, identities of all current signatories should be taken for verification.

5.12 KYC for corporate registered abroad

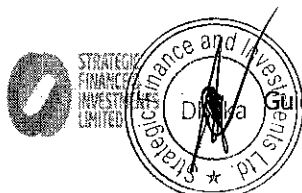
Particular care should be exercised when establishing business relationships with companies incorporated or registered abroad, or companies with no direct business link to Bangladesh. Such companies may be attempting to use geographic or legal complication to interpose a layer of opacity between the source of funds and their final destination. In such circumstances, institutions should carry out effective checks on the source of funds and the nature of the activity to be undertaken during the proposed business relationship. This is particularly important if the corporate body is registered or has known links to countries without anti-money laundering legislation and procedures equivalent to Bangladesh.

5.13 KYC for partnerships and other entities

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

5.14 Powers of attorney/mandates to operate accounts

Confirm the identities of holder of power of attorney/mandate or the guarantor of any customer's account and must be supported with the resolution or valid deed, as the case may be. The records of



all transactions undertaken in accordance with a power of attorney/mandate should be done with due care and record should be kept safely.

5.15 Transaction monitoring process

The nature of this monitoring will depend on the nature of customer's business. The purpose of monitoring of customer's business is to identify any significant changes or inconsistencies in the pattern of transactions.

Possible areas to monitor could be:

- i. Transaction type;
- ii. Frequency of transaction;
- iii. Unusual large transaction;
- iv. Geographical origin/destination of transaction;
- v. Changes in authorized signatories;
- vi. Borrower settling "problem" loans by large amounts of cash suddenly with no reasonable explanation of funds/source; etc.

5.16 What to do if customer due diligence (CDD) will not possible

In case where CDD cannot be done due to non-cooperation by the customer and/or if the information provided is found uncertain/suspicious after assessment, SFIL may take the following actions:

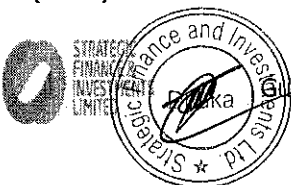
- i. SFIL shall not open account of such customer or may close existing account, if appropriate; and
- ii. Before closure of such accounts, approval from top management is necessary and the account holder shall be informed via notice detailing the reason behind such closure of account.

STR/SAR may be proceeded to Bangladesh Financial Intelligence Unit (BFIU) when there is a reasonable ground to do so.

A standard KYC format has been attached at "**Annexure-D**" with the guidelines which have been prepared on the basis of template provided by BFIU towards introduction of Uniform Account Opening Form for FIs.

5.17 Politically Exposed Persons (PEPs) and Influential Persons (IPs)

PEPs (as well as their family members and persons known to be close associates) are required to be subject to undertake enhanced due diligence by a reporting organization in general. This is because international standards issued by the FATF recognize that PEP may be in a position to abuse their public office, political power for private gains and PEP may use the financial system to launder the illicit gains. As FATF says „these requirements are preventive (not criminal) in nature, and should not be interpreted as stigmatizing PEPs as such being involved in criminal activity. The FATF has categorized PEPs into 3 (three) criteria which include:



- Foreign PEPs;
- Domestic PEPs (known as Influential Persons: IPs in Bangladesh) and
- Chief or similar high-ranking positions in an international organization.

It is important to note that only foreign PEPs automatically should be treated as high risk and therefore a reporting organization should conduct Enhanced Due Diligence (EDD) in this scenario. However, EDD should be undertaken in case of domestic PEPs (Influential Persons: IPs) and PEPs of the international organization when such customer relationship is identified as higher risk.

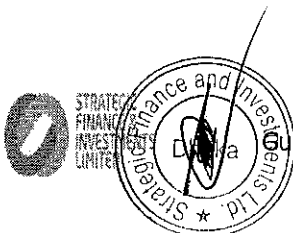
5.17.1 Who are Politically Exposed Persons (PEPs)

As per guidance notes on Politically Exposed Persons (PEPs) for all Reporting Organizations, A politically exposed person (PEP) is defined by the FATF as an individual who is or has been entrusted with a prominent public functions which include individuals in foreign country and domestic level. So, PEPs as per the FATF Standards and IPs as per Bangladeshi regulations, are the following individuals but not limited to-

- Heads of state or government, ministers and deputy or state ministers;
- Members of parliament or of similar legislative bodies;
- Members of the governing bodies of political parties (generally only apply to the national governing bodies where a member has significant executive power, e.g. over the selection of candidates or distribution of significant party funds);
- Senior politicians
- Members of supreme courts, of constitutional courts or of any judicial body the decisions of which are not subject to further appeal except in exceptional circumstances;
- Members of courts of auditors or of the boards of central banks;
- Ambassadors, Charges affairs and high-ranking officers in the armed forces;
- Head or the senior executives or members of the administrative, management or supervisory bodies or State-owned enterprises;
- Chief, directors, deputy directors and members of the board or equivalent function of an international organizations

5.17.2 Chief or similar high-ranking positions in an international organization.

Persons who are or have been entrusted with a prominent function by an international organization refers to members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions.



5.17.3 Who should be considered a family member of a PEP?

Family members of a PEP shall include:

- Spouse, or civil partner
- Children and their spouses or civil partner
- Parents

However, this is not an exhaustive list. Reporting organizations should take a proportionate and risk-based approach to the treatment of family members who do not fall into this definition. A corrupt PEP may use members of his/her wider family to launder the proceeds of corruption on his/her behalf. It may be appropriate to include a wider circle of family members (such as aunts and uncles) in cases where a reporting organization assessed a PEP to pose a higher risk. This would not apply in relation to lower risk PEPs. In low-risk situations, a reporting organization should not apply any EDD measures to someone who is not within the definition above and should apply normal customer due diligence measures. A family member of a PEP is not a PEP themselves purely as a consequence of being associated with a PEP.

5.17.4 Close associates' of a PEP

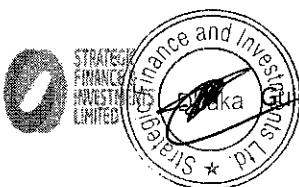
A known close associate" of a PEP is defined as:

- An individual known to have joint beneficial ownership of a legal entity or a legal arrangement or any other close business relationship with a PEP
- An individual who has sole beneficial ownership of a legal entity or a legal arrangement that is known to have been set up for the benefit of a PEP

A 'known close associate' of a PEP is not a PEP themselves purely as a consequence of being associated with a PEP.

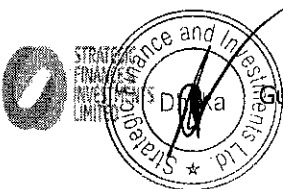
5.18 What are reporting organizations' obligations under the Regulations?

- The Regulations require reporting organizations to have in place appropriate risk-management systems and procedures to determine whether a customer or the beneficial owner of a customer is a PEP (or a family member or a known close associate of a PEP) and to manage the risks arising from the reporting organization's relationship with those customers. This includes where a PEP, family member or close associate is operating via an intermediary or introducer (this may include others in the regulated sector such as banking staff, lawyers, estate agents etc.). There are many legitimate reasons for doing so (e.g. a solicitor acting in a property transaction). In these situations, and in line with FATF guidance, BFIU expects reporting organizations to understand as part of their due diligence why a PEP, family member or close associate is using such an arrangement and use that as part of their assessment of risk.
- The Regulations state that in determining whether these systems and procedures are appropriate,



a reporting organization should refer to:

- Its own risk assessment of the money laundering/terrorist financing risks;
 - An assessment of the extent to which the risk would be increased by a business relationship with a PEP, family member or close associate. BFIU would expect that this is a case-by-case assessment and not an automatic assessment that a relationship creates a high risk of money laundering; and
 - Any information provided by the BFIU. This will include the BFIU's publication, thematic reviews, speeches on financial crime issues, BFIU's annual report.
- Where a reporting organization has identified that a customer (or beneficial owner of a customer) does meet the definition of a PEP (or a family member or known close associate of a PEP), the reporting organization must assess the level of risk associated with that customer and, as a result of that assessment, the extent to which enhanced due diligence measures need to be carried out. The risk factors set out in this guidance will help reporting organization to consider relevant factors when meeting these obligations. A reporting organization's assessment and its decision to apply relevant enhanced due diligence measures need to be clearly documented.
 - BFIU expects reporting organizations to make use of information that is reasonably available to them in identifying PEPs, family members or known close associates. This could include the following:
 - Public domain information such as websites of the governments, reliable news sources and work by reputable pressure groups focused on corruption risk. Reporting organizations should use a variety of sources where possible.
 - In line with the nature and size of the reporting organization, it may choose, but is not required, to use commercial databases that contain lists of PEPs, family members and known close associates. A reporting organization choosing to use such lists would need to understand how such databases are populated and will need to ensure that those flagged by the system fall within the definition of a PEP, family member or close associate as set out in the Regulations and this guidance.
 - BFIU expects that a reporting organization will not decline or close a business relationship with a person merely because that person meets the definition of a PEP (or a family member of a PEP or known close associate of a PEP). A reporting organization may, after collecting appropriate information and completing its assessment, conclude the risks posed by a customer are higher than they can effectively mitigate; only in such cases it will be appropriate to decline or close that relationship.
 - If, having assessed the risk associated with the customer and decided on an appropriate level of enhanced due diligence measures in line with this guidance, a reporting organization is unable to apply those measures, a reporting organization needs to comply with the requirement not to establish, or to terminate, a business relationship.
 - The following measures should be taken where a customer meets the definition of a foreign PEP, IPs/Chief of International Organization posing higher risk or a family member or known close



associate of a foreign PEP, IPs/Chief of International Organization posing higher risk:

- Obtain senior management approval for establishing or continuing business relationships with such persons
- Take adequate measures to establish the source of wealth and source of funds that are involved in business relationships or transactions with such persons
- Conduct enhanced, ongoing monitoring of those business relationships

The nature and extent of this due diligence should be appropriate to the risk that the reporting organization has assessed in relation to the customer. A reporting organization should apply more extensive measures for relationships assessed as high risk and less extensive measures for lower risk customers.

5.19 Ongoing monitoring of accounts and transactions

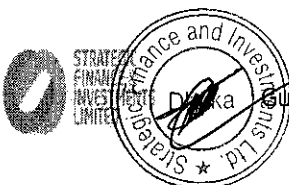
Effective internal control system may reduce the risk if relationship managers have an understanding of normal and reasonable account activity of their customers so that they have a means of identifying transactions which fall outside the regular pattern of an account's activity. Without such knowledge,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

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

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

SFIL has developed clear standards on what records must be kept for customer identification and individual transactions and their retention period. As the starting point and natural follow-up of the identification process, SFIL should obtain customer identification papers and retain copies of them for at least 5 (five) years after an account is closed.

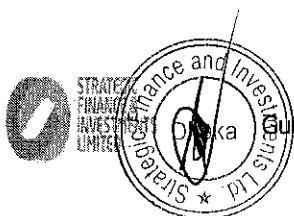


Chapter 6 : Know your employee (KYE)

Know Your Employee (KYE) program means the process to understand an employee's background, conflicts of interest and susceptibility to money laundering complicity. For appropriate management of KYE policies, procedures, internal controls, job description, code of conduct/ethics, levels of authority, compliance with personnel laws and regulations, accountability, dual control and other deterrents should be firmly in place.

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

A standard KYE format has been attached herewith at "**Annexure-E**". The data provided by each employee in KYE form shall be reviewed at least once in a year.



Chapter 7 : Compliance requirement of Strategic Finance & Investments Limited against ML/TF

The compliance requirements of FIs have been specified in Master Circular #12, dated: June 29, 2015 by Bangladesh Financial Intelligence Unit (BFIU). In this regard, Money Laundering Prevention (Amendment) Act, 2015 and Anti-Terrorism (Amendment) Act, 2013 and to be amended from time to time should also to be followed meticulously. The compliance requirement shall be documented and communicated to all levels of the employees of SFIL to develop awareness against ML/TF and to prevent ML and combat TF. As part of its AML/CFT policy, CCU with assistance of the top management shall communicate clearly too all employees on annual basis through a statement from the Managing Director & CEO stating SFIL's position against ML/TF and criminal activities.

A. Domestic requirement

7.1 Compliance requirement under domestic law

According to section 25(1) of Money Laundering Prevention (Amendment) Act, 2015 the responsibilities and other obligations prescribed by law of SFIL in prevention of money laundering are:-

- a) To maintain complete and correct information with regard to the identity of its customers during the operation of their accounts;
- b) If any account of a customer is closed, to preserve account and previous records of transactions of such account for at least 5(five) years from the date of such closure;
- c) To provide with the information maintained under clauses (a) and (b) to Bangladesh Financial Intelligence Unit (BFIU) from time to time, on its demand;
- d) If there be any doubtful transaction or attempt of such transaction as defined under clause (n) of section 2 of Money Laundering Prevention (Amendment) Act, 2015 the matter shall be reported as "suspicious transaction report" to the BFIU immediately.

7.2 Board approved guidelines for preventing ML and combating TF

In pursuance of section 16(2) of Anti-Terrorism (Amendment) Act, 2013, and Bangladesh Financial Intelligence Unit Master circular#12, dated: June 29, 2015, all FIs must have their own policy manual duly approved by their Board of Directors/topmost committee to prevent ML and combat TF. This policy manual must be in conformity with international standard and laws and regulations in force in Bangladesh and circulars issued by BFIU from time to time. The guidelines shall be circulated among all the concerned employees for information and necessary action to prevent ML and combat TF. FIs shall from time to time review and confirm meticulous compliance of the circulars issued by BFIU or Government through official gazette.



7.3 Appointment of CAMLCO, DCAMLCO and BAMLCO

To implement the policy manual and compliance of instructions of Bangladesh Financial Intelligence Unit (BFIU), SFIL should:

- i. Designate one high level officer as Chief Anti-Money Laundering Compliance Officer (CAMLCO) and a senior level officer as DCAMLCO in the Central Compliance Unit (CCU); and
- ii. Designate one officer as Branch Anti-Money Laundering Compliance Officer (BAMLCO) at branch level.

7.4 Customer identification

SFIL should mandatorily collect complete information and identification of customers and verify their correctness to keep themselves free from ML/TF risks. As per BFIU master circular#12/2015, a customer is defined as:

- i. Any person or institution maintaining an account of any type with a FIs or having business relationship with FIs;
- ii. The person or institution as true beneficial owner in whose favor the account is operated;

the trustee, intermediary or true beneficial owner of the transaction of the accounts operated by the trust and professional intermediaries (such as lawyer/law firm, chartered accountant, etc.) under the existing legal infrastructure;

7.5 Other measures

The following measures also to be taken under compliance requirement against ML/TF:

- a) How to conduct CDD/EDD at different stages like- while establishing relationship with the customer or conducting financial transaction with the existing customer;
- b) To be sure about the customer's identity through collection of adequate information towards satisfaction of the concerned employee i.e. doing CDD;
- c) To be satisfied while operating any account by a person on behalf of the customer that the person has due authorization to operate the account and in this case correct and complete information of the person must be collected before opening/operating such account or transaction;
- d) Legal status and accuracy of information of the accounts operator/s are shall be ascertained while any account is to operate by trustee and professional intermediaries i.e. lawyers/law firm, chartered accountants, etc.;
- e) Enhanced due diligence (EDD) shall have to be ensured with a person of the countries and territories that do not meet international standard in preventing ML/TF i.e. countries and



territories listed as high risk country in FATF's public statements while establishing and maintaining business relationship and conducting financial transaction;

- f) In case of beneficial owner (i.e. the customer has controlling share of a company or/and holds 20.00% or more shares of a company) of an account, SFIL shall have to collect and ensure:
 - i. Complete and correct information of identity of the persons besides the customer;
 - ii. Controller or the owner of the customer; and
 - iii. Complete and correct information of identity of the beneficial owners shall have to be collected and preserved.

7.6 What to do in case of PEPs and IPs while opening and/or operating account

While opening and/or operating account or at the time of financial transaction of PEPs/IPs, EDD shall have to be exercised. Following instructions shall have to be followed to ensure EDD:

- i. SFIL shall identify risks associated for opening and operating such accounts of PEPs/IPs;
- ii. Take reasonable measures to ensure source of wealth and source of funds;
- iii. Ongoing transactions monitoring process shall have to be done by the concerned officer; and
- iv. All formalities shall have to be complied as per Foreign Exchange Regulation Act-1947 (as amended in 2018) while opening and operating accounts of non-resident PEPs/IPs;
- v. KYC shall be reviewed on a regular interval basis or at least once in a year etc.

All instructions as detailed for PEPs/IPs shall be equally applicable if business relationship is established with family members and close associates of these persons who may pose reputational risk to SFIL. The above instructions shall also be applicable to customers or beneficial owners who become PEPs/IPs after business relationship have been established.

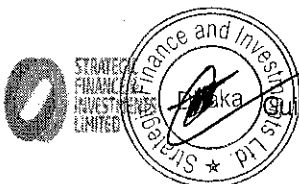
7.7 Appointment and training

7.7.1 Employee screening

To prevent ML and combat TF, SFIL shall have to undertake proper screening mechanism in appointment procedures so that ML/TF risks could be avoided.

7.7.2 Employee training

To ensure proper compliance of ML/TF activities of SFIL shall arrange suitable in-house or outdoor training of officials on preventing of ML and combating TF.



7.8 Awareness of customers regarding ML/TF

At the time of opening or operating an account and/or doing KYC, concerned officer shall explain to the customers the reasons and/or grounds for asking documents or identities. The concerned officer shall also respond to the customer's query, if any. The Management of SFIL may distribute leaflets among customers to make them aware of ML/TF and also arrange to stick posters in visible place at Head Office or every branch.

SFIL also requires to display trailer, documentary etc. in public or other media to make awareness under Corporate Social Responsibility with due approval of the competent authority.

7.9 Suspicious transaction report (STR)/suspicious activity report (SAR)

According to the provision of section 25(1) (d) of Money Laundering Prevention (Amendment) Act, 2015 and section 2(16) of Anti-Terrorism (Amendment) Act, 2013, SFIL requires to submit report proactively and immediately to Bangladesh Financial Intelligence Unit (BFIU) on suspicious, unusual or doubtful transactions/activity report relating to ML/TF. (More details are in Chapter-10).

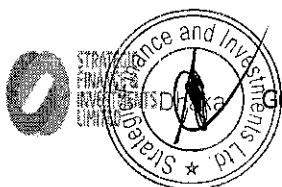
7.10 Cash transaction report (CTR)

According to the provision of section 23 of Money Laundering Prevention (Amendment) Act, 2015 and section 15 of Anti-Terrorism (Amendment) Act, 2013 and on the basis of BFIU Master Circular#12, dated June 29, 2015, SFIL requires to submit CTR to Bangladesh Financial Intelligence Unit (BFIU) on monthly basis on or before 21st of the next month using GoAML software on doubtful cash transactions, if any, relating to ML/TF. (More details are in Chapter-11).

7.11 Procedure of Self-Assessment Report

This policy requires that appropriate and timely self-assessments, tests, audits and evaluations shall be conducted to ensure that the SFIL is in compliance with the regulations. Each and every branch shall assess their performance through self-assessment report on half yearly basis according to Master Circular # 12 dated: June 29, 2015 of the Bangladesh Financial Intelligence Unit (BFIU). This procedure enables management to identify areas of risk or to assess the need for additional control mechanisms. The SAR should conclude with a report documenting the work performed, how it has been controlled/supervised and the resulting findings, conclusions and recommendations. The SAR should advise management whether the internal procedures and statutory obligations of SFIL have been properly discharged. Each branch will assess its AML/CFT activities covering the following areas on half yearly basis and submit the report to CCU and ICC within next 15 (fifteen) days of each half year end:

- i. The percentage of officers/employees that received official training on AML/CFT;
- ii. The awareness of the officers/employees about the internal AML/CFT policies, procedures and programs, and BFIU's instructions, circulars and guidelines;
- iii. The arrangement of AML/CFT related meeting on regular interval;



- iv. The effectiveness of the customer identification during opening an individual, corporate and other account;
- v. The risk categorization of customers by the branch;
- vi. Regular update of customer profile upon reassessment;
- vii. The monitoring of customers' transactions;
- viii. Identification of Suspicious Transaction Reports/Suspicious Activity Report (STRs/SARs);
- ix. The maintenance of a separate file containing MLPA, circulars, training records, reports and other ML related documents and distribution of those among all employees;
- x. The measures taken by the branch during opening of account of PEPs/IPs;
- xi. Consideration of UNSCR 1267 and 1373 while conducting any business; and
- xii. The compliance with AML/CFT weaknesses/irregularities, as the CCU/ICC of Head Office and BFIU's inspection report mentioned.

A standard self-assessment report format has been attached at "**Annexure-F**" of this guidelines as prescribed in Master Circular #12 dated June 29, 2015 of the BFIU.

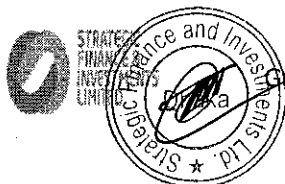
7.12 Independent testing procedures (ITP)

As per Master Circular # 12 dated: June 29, 2015 of the Bangladesh Financial Intelligence Unit (BFIU) testing on Prevention of Money Laundering is to be conducted on the branches by the internal audit personnel of ICC department and by an outside party such as the institution's external auditors. While conducting the same, they should also look into whether the directives of BFIU issued from time to time in this respect are followed meticulously by the branches.

Mentionable that compliance of AML is the responsibility of each employee of SFIL. Therefore, all guidelines related to AML be updated as and when required and circulated to ensure that all employees are aware of the Money Laundering Prevention (Amendment) Act, 2015 and Anti-Terrorism (Amendment) Act, 2013, BFIU's instructions, internal guidelines and other policies and procedures.

The test will cover the following areas:

- i. Activities of branch compliance unit/BAMLCO;
- ii. Knowledge of officers/employees on AML/CFT issues;
- iii. Know Your Customer Identification (KYC) process;
- iv. Process and action to identify STRs/SARs/CTRs;



- v. Regular submission of reports to CCU;
- vi. Proper record keeping; and
- vii. Overall AML/CFT related activities by the branch.

The tests include interviews with employees handling transactions and interviews with their supervisors to determine their knowledge and compliance with Company's AML/CFT procedures like:

- i. Sampling of large transactions followed by a review of transaction record retention forms and suspicious transaction referral forms;
- ii. Test of the validity and reasonableness of any exemption granted by the FI; and
- iii. 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.

A standard ITP format has been attached at "**Annexure-G**" of this guidelines as prescribed in Master Circular #12 dated June 29, 2015 of the BFIU.

7.13 Overall assessment report

In compliance with the Master Circular # 12, dated: June 29, 2015 of Bangladesh Financial Intelligence Unit (BFIU), the Central Compliance Unit of SFIL requires to prepare an Overall Assessment Report on half yearly basis towards submission to the BFIU stating direction/recommendation, if any, of the Board or Top Management Committee.



Chapter 8 : Compliance program of Strategic Finance & Investments Limited against ML/TF

SFIL considering the prevailing laws and regulations; and Bangladesh Financial Intelligence Unit (BFIU)'s Circulars should establish and maintain an effective AML/CFT program which should include the followings:

- i. Development of internal policies, procedures and controls mechanism;
- ii. Appointment of an AML/CFT compliance officer;
- iii. Ongoing employee training programs; and
- iv. Independent audit functions including internal and external audit functions to test AML/CFT programs.

The compliance policies should be documented, approved by the Board of Directors and communicated to all levels of the organization.

8.1 Formation of central compliance unit (CCU)

As per Bangladesh Financial Intelligence Unit (BFIU) instructions, the CCU will be headed by a senior level employee whose position cannot be lower than the third rank in seniority of organizational hierarchy and a minimum of 7 (seven) years of working experience, with a minimum of 3(three) years at the managerial level/administrative level. The CAMLCO of the Company will be the Head of the CCU. S/he will be assisted by DCAMLCO & three other designated officers among which two will be from business department and another from any suitable department but none from the ICC department. The organogram of CCU is shown below:

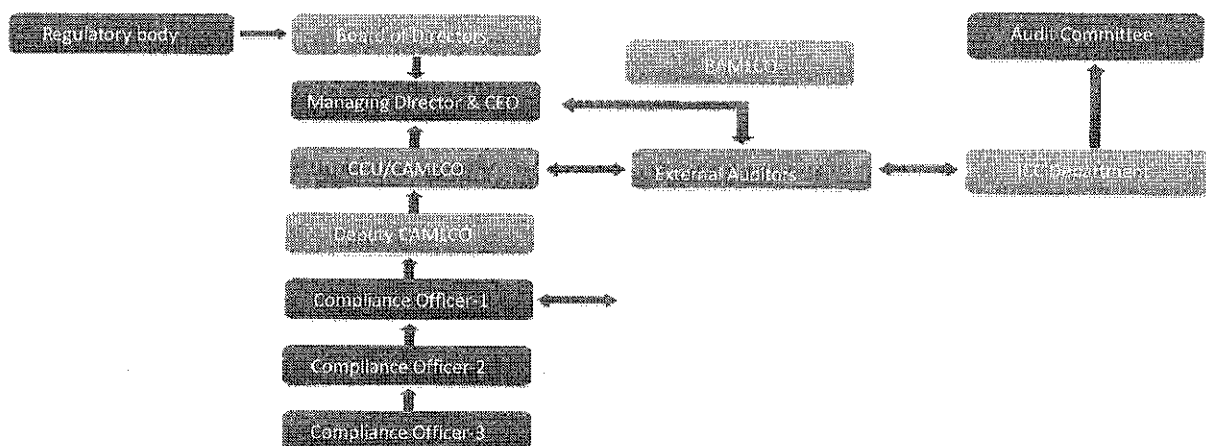


Figure: Formation of Central Compliance Unit

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

CCU will issue the instructions to be followed by the branches; these instructions will be prepared on

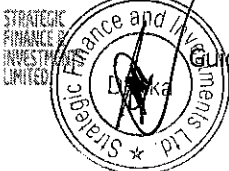


the basis of combination of issues in monitoring of transactions, internal control, policies and procedures from the point of view of preventing money laundering & combating terrorist financing.

8.2 Responsibilities of the officials of SFIL

The responsibilities of the officials various departments are presented below on tabular form for easy understanding of and smooth implementation by the concerned employee/s:

| Responsible Depart. Or Officials | Responsibilities |
|--|---|
| Officer in charge who is responsible for opening new accounts/making transaction | <ul style="list-style-type: none"> a. To interview the potential customer; b. Verify customer profile; c. To arrive at threshold limit for each account (new as well as existing) and to exercise due diligence in identifying suspicious transactions/activities; d. To restrict opening of accounts in the name of terrorist/banned organizations; e. To adhere with the provisions of Money Laundering Prevention (Amendment) Act, 2015; and f. To comply with the guidelines issued by Bangladesh Financial Intelligence Unit (BFIU) and by the company from time to time in respect of opening and conduct of account. |
| Chief Risk Officer | To assess the ML risk involves in operating activities of the Company and to evaluate adequacy and effectiveness of the control mechanism set for safeguarding the company's risks. |
| Head of Operations | <ul style="list-style-type: none"> a. To scrutinize and ensure that the information furnished in the account opening form/customer profile/threshold limit are in strict compliance with AML/CFT Guidelines before authorizing opening of account; and b. To certify regarding compliance with AML/CFT Guidelines and report suspicious transactions to CAMLCO/Managing Director & CEO. |
| Internal Auditor | To verify and record his comments on the effectiveness of measures taken by the concerned officials and the level of implementation AML/CFT Guidelines. |
| CAMLCO | <ul style="list-style-type: none"> a. To implement and enforce Company's AML policies; b. To ensure sending STR/SAR/CTR to BFIU; c. To inform DCAMLCO/BAMLCO required actions, if any, to be taken. |
| DCAMLCO | <ul style="list-style-type: none"> a. To assist CAMLCO to implement and enforce Company's AML policies; b. Send STR/SAR/CTR to BFIU through CCU; c. Ensuring flow of information to BAMLCO towards reporting to CAMLCO and CCU; and |
| BAMLCO | <ul style="list-style-type: none"> a. Ongoing monitoring of customer's KYC profile/CDD/EDD and transaction activities; b. Report STR/SAR/CTR through branch manager to CAMLCO and CCU; c. Provide AML training to branch employees; |



| | |
|-------------------------|---|
| | <ul style="list-style-type: none"> d. Communicate and update to all employees in case of any changes in national or Company's own policies; e. Organize a meeting with all executives/officers at least once after each quarter end as per Master Circular#12/2015 of Bangladesh Financial Intelligence Unit (BFIU); and f. Submit Self-Assessment Report to CAMLCO/CCU/ICC. |
| Branch Manager | <ul style="list-style-type: none"> a. Ensure that the AML program is effective within the Branch; b. Overall responsibility to ensure that the Branch has an effective AML program in place and that it is working effectively. |
| Top Management | Prompt reporting of information regarding suspicious transactions to concerned law enforcing authority in consultation with the competent authority/ies. |
| Managing Director & CEO | Overall responsibility to ensure that SFIL has AML program in place and that it is working effectively. |

8.3 The responsibilities of CCU members

To ensure compliance of the Money Laundering Prevention (Amendment) Act, 2015 and Anti-Terrorism (Amendment) Act, 2013, SFIL requires to establish a Central Compliance Unit (CCU) to arrange internal monitoring and control under the leadership of a high official at the Head Office whose seniority shall not be less than third from the official hierarchy. CCU will issue the instructions to be followed by each concerned officer of Head Office as well as branch/es; these instructions will be prepared on the basis of combination of issues in monitoring of transactions, internal control, policies and procedures from the point of view of preventing ML and combating TF. CCU shall be dedicated solely to perform the compliance functions. The responsibilities of a CCU shall include:

- i. Preparing an overall assessment report after evaluating the self-assessment reports received from the branches and submitting it with comments and/or recommendations to the Managing Director & CEO;
- ii. Preparing an assessment report on the basis of the submitted checklist of inspected branches by ICC department; and
- iii. Submitting a half-yearly overall assessment report to BFIU within 60 (sixty) days after end of each half year as per Bangladesh Financial Intelligence Unit (BFIU) Master Circular # 12/2015.

8.4 Appointment of Chief Anti-Money Laundering Compliance Officer (CAMLCO)

SFIL requires to designate a Chief AML/CFT Compliance Officer (CAMLCO) at its Head Office who has sufficient authority to implement and enforce corporate-wide AML/CFT policies, procedures and measures. The CAMLCO will directly report to the Managing Director & CEO for his/her responsibility. The CAMLCO will also be responsible to coordinate and monitor day to day compliance with applicable AML/CFT related laws, rules and regulations as well as with its internal policies, practices, procedures



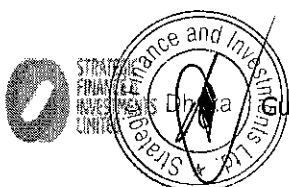
and controls.

The CAMLCO will be the head of CCU and s/he will be the central point of contact for communicating with the regulatory and/or investigation agencies regarding issues related to Company's AML/CFT program. The position of the CAMLCO cannot be lower than the third rank in seniority of organizational hierarchy. The CAMLCO should have a minimum of 7 (seven) years of working experience, with a minimum of 3 (three) years at a managerial/administrative level.

8.5 Responsibilities of CAMLCO

The major responsibilities of CAMLCO are as follows:

- i. To monitor, review and coordinate application and enforcement of AML/CFT 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 or activities, and a written AML/CFT training plan;
- ii. To monitor changes of laws/regulations and directives of Bangladesh Financial Intelligence Unit (BFIU) and revise its internal policies accordingly;
- iii. To respond to compliance questions and concerns of the staff and advise branches/units and assist in providing solutions to potential issues involving compliance and risk;
- iv. To ensure that Company's AML/CFT policy is complete and up-to-date, to maintain ongoing awareness of new and changing business activities and products;
- v. To develop compliance knowledge of all staff, especially the compliance personnel and conduct training courses in this regard;
- vi. To develop and maintain ongoing relationships with regulatory authorities, external and internal auditors, regional/branch/unit heads and compliance resources to assist in early identification of compliance issues;
- vii. To assist in review of control procedures in SFIL to ensure legal and regulatory compliance and in the development of adequate and sufficient testing procedures to prevent and detect compliance lapses, if any;
- viii. To monitor the business through self-testing for AML/CFT compliance and take any required corrective action;
- ix. To manage the STR/SAR/CTR process by:
 - a. Reviewing transactions referred by branch or unit compliance officers as suspicious through CCU meeting;
 - b. Reviewing the transaction monitoring reports (directly or together with account management personnel);



- c. Ensuring STR/SAR/CTR as the case may be:
 - Are prepared when appropriate;
 - Are accompanied by documentation of the branch's decision to retain or terminate the account as required under its policy;
 - Are advised branch/es of SFIL who are known to have a relationship with the customer; and
 - Are reported to the Managing Director & CEO, and the Board of Directors when the suspicious activity is judged to represent significant risk to the institution, including reputation risk.
- d. Ensuring that a documented plan of corrective action, appropriate for the seriousness of the suspicious activity, be prepared and approved by the branch manager;
- e. 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; and
- f. Managing the process for reporting suspicious activity to BFIU after appropriate internal consultation.

8.6 Responsibilities of deputy CAMLCO

The major responsibilities of deputy CAMLCO are as follows:

- i. Assisting CAMLCO in implementing and enforcing institution's AML/CFT policies;
- ii. Send STR/SAR/CTR to Bangladesh Financial Intelligence Unit (BFIU) through CCU;
- iii. Ensuring flow of information to BAMLCO towards reporting to CAMLCO and CCU; and
- iv. To assist CAMLCO to take other required actions, if any, to be taken.

8.7 Responsibilities of BAMLCO

SFIL requires designating Branch Anti-money Laundering Compliance Officer (BAMLCO) at every branch. BAMLCO will be the second man of a branch and have a minimum 3 (three) year experience in related field. The responsibilities of a BAMLCO are as follows:

- i. Ongoing monitoring of customer's KYC profile/CDD/EDD and transaction activities;
- ii. Report any STR/SAR/CTR through branch manager to CAMLCO and CCU;
- iii. Provide AML training to branch employees;
- iv. Communicate and update to all employee in case of any changes in national or Company's own policy;
- v. Organize a meeting with all executives/officers at least once after each quarter end as per Master Circular#12/2015 of Bangladesh Financial Intelligence Unit (BFIU); and
- vi. Submit Self-Assessment Report and applicable returns to CAMLCO/CCU/ICC, as the case may be, on timely manner.



8.8 Employee training and awareness program

As per FATF recommendation no.18, a formal AML/CFT compliance program should include an ongoing employee training schedule. The importance of a successful training and awareness program cannot be overstated. Employees in different business functions need to understand how the financial institution's policy, procedures, and controls affect them in their day to day activities. As per the Master Circular #12 dated June 29, 2015, SFIL shall have to arrange suitable training for officials to ensure proper compliance of AML/CFT activities. Following training procedures to be followed by the Company for prevention of ML and combating TF:

8.8.1 Employee awareness

Employee must be aware of their own personal statutory obligations and that they will be personally liable for failure to report information in accordance with internal procedures. All employees must be trained to co-operate fully and to provide a prompt report of any STR/SAR/CTR.

8.8.2 Education and training programs

All relevant employees should be educated in the process of the KYC requirements to prevent ML and & combating TF. 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. Concerned employees should be alert to any change in the pattern of a customer's transactions or circumstances that might constitute criminal activity.

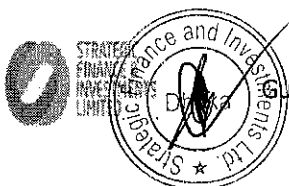
Generally all trainings could be divided in two types:

- i. General training; and
- ii. Job specific training

General training

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

- i. General information on the risks of ML and TF schemes, methodologies, and typologies;
- ii. Legal framework, how AML/CFT related laws apply to SFIL;
- iii. Policies and systems with regard to customer identification and verification, due diligence, monitoring;
- iv. How to react when faced with a suspicious customer or transaction;
- v. How to respond to customers who want to avoid reporting requirements;
- vi. Stressing the importance of not tipping off customer information;
- vii. STR/SAR/CTR requirements and processes; and
- viii. Duties and accountabilities of employees.



Job Specific Training

New employee training

For a new employee the compliance policy statement must be signed-off at the beginning of the joining and he/she must have an on the job training from the departmental head regarding the importance of AML/CFT activities. The new employee must also go through the yearly training on AML/CFT.

a) Customer service/relationship managers

Employees of the investment departments who are to deal 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 to fight against ML and TF. They must be made aware of their legal responsibilities and 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.

b) Operation department

Operation department employee who receives loan application forms and cheques for deposit into company's account should receive training on the processing and verification procedures of customer profile/CDD/EDD. In addition, they need to be trained on the organization's account opening and customer verification procedures. Employee should be aware that the offer to deploy suspicious funds or the request to undertake a suspicious transaction may need to be reported to the CAMLCO (or alternatively a line supervisor).

c) 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.

d) Audit and compliance officer

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

e) Senior management commitment and role of the Board of Directors

The most important element of a successful AML/CFT program is the commitment of senior management, including the Managing Director & CEO and the Board of Directors. AML/CFT issues may be communicated to the Board from time to time, if necessary. The message from top management and the Board of Directors will be "Zero Tolerance" in case of AML and CFT.



f) AML/CFT compliance officer

The AML/CFT compliance officer should receive in depth training in all aspects of the AML/CFT legislation, Bangladesh Financial Intelligence Unit (BFIU) directives, circulars, guidelines and internal policies. In addition, the AML/CFT Compliance Officer will require extensive instructions on the validation and reporting of STR/SAR/CTR and on the feedback arrangements, and on new trends and patterns of criminal activities.

8.8.3 Independent audit function

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

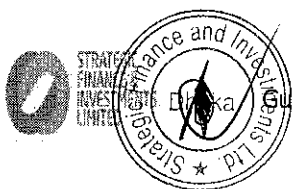
8.8.3.1 Internal Auditors'

The responsibilities of internal auditors are:

- a. Address on the adequacy of AML/CFT risk assessment;
- b. Examine/attest the overall integrity and effectiveness of the management systems and the control environment;
- c. Examine the adequacy of Customer Due Diligence (CDD) policies, procedures and processes, and whether they comply with internal requirements;
- d. Perform appropriate transaction testing with particular emphasis on high risk operations (products, service, customers, regulatory and geographic locations);
- e. Assess the adequacy of the SFIL processes for identifying and reporting STR/SAR/CTR; communicate the findings to the CCU/Managing Director & CEO and/or Board in a timely manner;
- f. Track previously identified deficiencies and ensures that management corrects them;
- g. Assess training adequacy, including its comprehensiveness, accuracy of materials, training schedule and attendance tracking;
- h. Employee accountability for ensuring AML/CFT compliance;
- i. Effectiveness of training, in view of specific risks of individual business lines; etc.

8.8.3.2 External Auditors'

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 auditors should focus their audit programs on risk factors and conducts intensive reviews of higher risk areas where controls may be deficient. SFIL may, if requires, facilitate the external auditors in reviewing whether the ML policies have been complied or not by the management.



Chapter 9 : Offence of money laundering and punishment

9.1 Offence

For the purpose of this Act money laundering shall be deemed to be an offence.

9.2 Punishment

According to section 25(2) of Money Laundering Prevention (Amendment) Act, 2015, if any reporting organization violates the directions mentioned in sub-section (1) of section 25 of Money Laundering Prevention (Amendment) Act, 2015, Bangladesh Financial Intelligence Unit (BFIU) or regulating authority of reporting organization may-

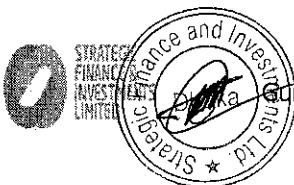
- a. Impose a fine of at least Taka 50(fifty) thousand but not exceeding Taka 25(twenty five) lacs on the reporting organization; and
- b. In addition to the fine mentioned in clause (a), cancel the license or the authorization for carrying out commercial activities of the said organization or any of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

In addition to the above mentioned provisions there are some provisions of penalties in section 23 of Money Laundering Prevention (Amendment) Act, 2015. These are:

Under section 23(3): If any reporting organization fails to provide with the requested information timely under this section, Bangladesh Financial Intelligence Unit (BFIU) may impose a fine on such organization which may extend to a maximum of Taka 5(five) lacs at the rate of Taka 10(ten) thousand per day and if any organization is fined more than 3 (three) times in 1(one) financial year, BFIU may suspend the registration or license of the organization or any of its branches, service centers, booths or agents for the purpose of closing its operation within Bangladesh or, as the case may be, shall inform the registration or licensing authority about the fact so that the relevant authority may take appropriate measures against the organization.

Under section 23(4): If any reporting organization provides with false information or statement requested under this section, Bangladesh Financial Intelligence Unit (BFIU) may impose a fine on such organization not less than Taka 20(twenty) thousand but not exceeding Taka 5 (five) lacs and if any organization is fined more than 3(three) times in 1 (one) financial year, BFIU may suspend the registration or license of the organization or any of its branches, service centers, booths or agents for the purpose of closing its operation within Bangladesh or, as the case may be, shall inform the registration or licensing authority about the fact so that relevant authority may take appropriate measures against the said organization.

Under section 23(5): If any reporting organization fails to comply with any instruction given by



Bangladesh Financial Intelligence Unit (BFIU) under this Act, BFIU may impose a fine on such organization which may extend to a maximum of Taka 5 (five) lacs at the rate of Taka 10 (ten) thousand per day for each of such non-compliance and if any organization is fined more than 3(three) times in 1(one) financial year, BFIU may suspend the registration or license of the organization or any of its branches, service centers, booths or agents for the purpose of closing its operation within Bangladesh or, as the case may be, shall inform the registration or licensing authority about the fact so that the relevant authority may take appropriate measures against the said organization.

Under section 23(6): If any reporting organization fails to comply with any order for freezing or suspension of transaction issued by Bangladesh Financial Intelligence Unit (BFIU) under clause (c) of sub- section 23(1) of Money Laundering Prevention (Amendment) Act, 2015, BFIU may impose a fine on such organization not less than the balance held on that account but not more than twice of the balance held at the time of issuing the order.

Under section 23(7): If any person or entity or reporting organization fails to pay any fine imposed by Bangladesh Financial Intelligence Unit (BFIU) under sections 23 and 25 of this Act, BFIU may recover the fine from accounts maintained in the name of the relevant person, entity or reporting organization in any bank or financial institution or BFIU, and in this regard if any amount of the fine remains unrealized, BFIU may, if necessary, make an application before the court for recovery and the court may pass such order as it deems fit.

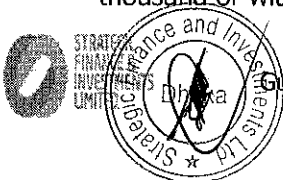
Under section 23(8): If any reporting organization is imposed fine under sub-sections 23 (3), (4), (5) and (6), Bangladesh Financial Intelligence Unit (BFIU) may also impose a fine not less than Taka 10 (ten) thousand but not exceeding Taka 5 (five) lacs on the responsible owner, directors, officers and staff or persons employed on contractual basis of that reporting organization and, where necessary, may direct the relevant organization to take necessary administrative action.

Under section 5: Punishment for violation of an order for freezing or attachment

Any person who violates a freezing or attachment order issued under this Act shall be punished with imprisonment for a term not exceeding 3(three) years or with a fine equivalent to the value of the property subject to freeze or attachment, or with both.

Under section 6: Punishment for divulging information

- a) No person shall, with an ill motive, divulge any information relating to the investigation or any other related information to any person, organization or news media.
- b) Any person, institution or agent empowered under this Act shall refrain from using or divulging 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.
- c) Any person who contravenes the provisions of sub-sections (1) and (2) 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.



Under section 7: Punishment for obstruction or non-cooperation in investigation, failure to submit report or obstruction in the supply of information

1. Any person who, under this Act-

- a) Obstructs or declines to cooperate with any investigation officer for carrying out the investigation; or
- b) Declines to supply information or submit a report being requested without any reasonable ground;

Shall be deemed to have committed an offence under this Act.

2. Any person who is convicted under sub-section (1) shall be punished with imprisonment for a term not exceeding 1(one) year or with a fine not exceeding Taka 25 (twenty five) thousand or with both.

Under section 8: Punishment for providing false information

- 1. No person shall knowingly provide false information in any manner regarding the source of fund or self-identity or the identity of an account holder or the beneficiary or nominee of an account.
- 2. Any person who violates the provision of sub-section (1) shall be punished with imprisonment for a term not exceeding 3(three) years or a fine not exceeding Taka 50(fifty) thousand or with both.

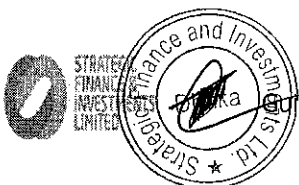
Under section 27: Offences committed by an entity

If any offence under this Act is committed by an entity, every proprietor, director, manager, secretary or any other officer, staff or representative of the said entity who is directly involved in the offence shall be deemed to be guilty of the offence, unless he is able to prove that the offence has been committed without his knowledge or he tried his best to prevent it.

Explanation: In this section "director" includes any member of the partnership entity or any of the Board of Directors of the entity, by whatever name called.

Under section 28: Protection of actions taken in good faith

No suit or prosecution or administrative measures or any other legal proceedings shall lie against the Government or any officer or staff of the Government or Bangladesh Financial Intelligence Unit (BFIU) or any officer or staff of BFIU or the Investigating Agency or any officer or staff of the Agency or any reporting organization or its Board of Directors or any of its officers or staff for anything which is done in good faith under this Act or Rules made thereunder for which any person is or likely to be affected.



Chapter 10 : Suspicious Transaction Report/ Suspicious Activity Report (STR/SAR)

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

According to the provision of section 25(1) (d) of Money Laundering Prevention (Amendment) Act, 2015 and 15(1) (a) of Anti-Terrorism (Amendment) Act, 2013 SFIL should report to Bangladesh Financial Intelligence Unit (BFIU) proactively and immediately, facts on suspicious, unusual or doubtful transactions likely to be related to ML/TF; because BFIU has the power to call STR/SAR from FIs related to ML/TF.

10.1 General definition

Generally STR/SAR means a formatted report of suspicious transactions/activities where there are reasonable grounds to suspect that funds are the proceeds of predicate offence or may be linked to terrorist activity or the transactions do not seem to be usual one. Such report is to be submitted by financial institutions to Bangladesh Financial Intelligence Unit (BFIU).

10.2 Legal definition

Under section (2) (z) of Money Laundering Prevention (Amendment) Act, 2015 "Suspicious Transaction" means such transactions-

- a) Which deviates from usual transactions;
- b) Of which there is ground to suspect that,
 - i. The property is the proceeds of an offence,
 - ii. It is financing to any terrorist activity, a terrorist group or an individual terrorist;
- c) 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 (Amendment) Act, 2013, STR/SAR refers to the transaction that relates to financing for terrorism or terrorist individual or entities.

One important thing may be noted that SFIL do not require to establish any proof of occurrence of a predicate offence; it is a must to submit STR/SAR only on the basis of suspicion.

10.3 Obligations of such report

As per the Money Laundering Prevention (Amendment) Act, 2015, SFIL is obligated to submit STR/SAR



to Bangladesh Financial Intelligence Unit (BFIU). Such obligation also prevails under Anti-Terrorism (Amendment) Act, 2013. Other than the legislation, BFIU has also instructed the FIs to submit STR/SAR through Master Circular # 12, dated June 29, 2015.

10.4 Reasons for reporting of STR/SAR

STR/SAR is very crucial for the safety and soundness of our institutions and accordingly SFIL should submit STR/SAR considering the followings:

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

10.5 Identification and evaluation of STR/SAR

Identification of STR/SAR is very crucial for SFIL to mitigate the risk. Identification of STR/SAR depends upon the detection mechanism in place. Such identification may not only take place at the time of transaction but also at the time of doing KYC/CDD/EDD and attempt to transaction or financial relation.

10.5.1 Identification of STR/SAR

Identification of STR/SAR shall be started by identifying unusual transactions and activities. Transactions may be unusual in terms of complexity of transaction, nature of transaction, volume of transaction, time of transaction etc. Concerned employee can take following steps to detect STR/SAR:

- i. Reviewing KYC profile;
- ii. Monitoring customer transactions; and
- iii. Using red flag indicator.

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



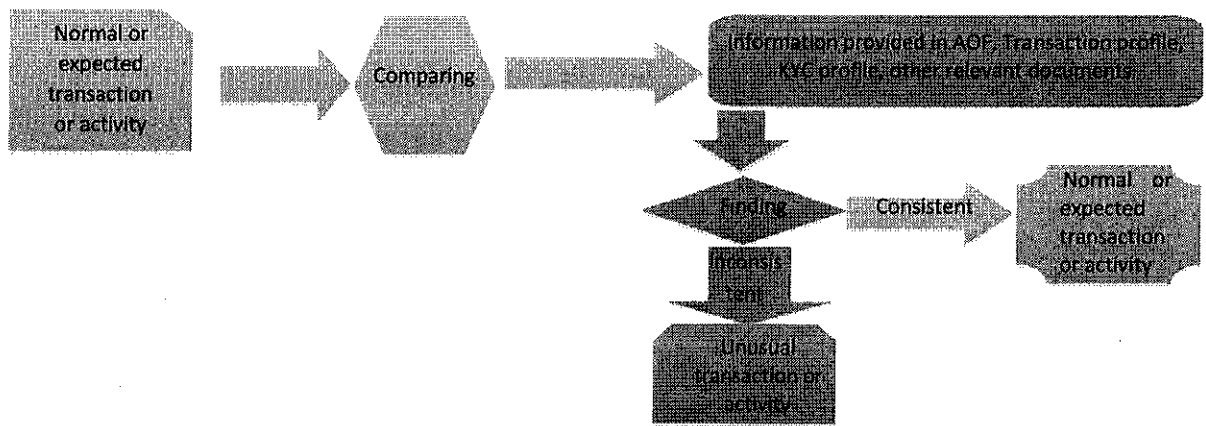


Figure: STR/SAR Identification Process

In case of reporting of STR/SAR, SFIL should conduct the following 3(three) stages:

a) Identification:

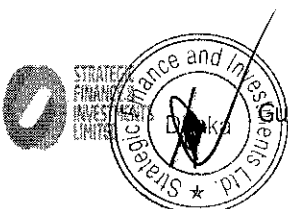
This stage is very vital for STR/SAR reporting. SFIL need to monitor constantly the activities of the accounts of customers. Monitoring mechanisms should be more rigorous in high-risk areas of an institution having alert management mechanism and appropriate staff (e.g. the AML/CFT compliance officer) dealing with of unusual/suspicious transactions or activities. Training of staff on the identification of unusual/suspicious activity should always be an ongoing process. SFIL must be vigilant in complying KYC meticulously and sources of funds of the customer to identify STR/SAR. (A standard format to process STR/SAR to CCU has been attached at "Annexure-H" of this guidelines).

a) Evaluation:

After identification of STR/SAR, compliance officer or BAMLCO should evaluate the transaction/activity by interviewing the customer or through any other means. In the evaluation stage concerned officer/BAMLCO must be tactful considering the tipping off provision of the acts. If they are not satisfied, they should forward the report to CCU. After receiving report from Head Office/branch CCU should also evaluate the report whether the STR/SAR report should be sent to BFIU or not. At every stage of evaluation SFIL should keep records complying the requirement of Money Laundering Prevention (Amendment) Act, 2015.

b) Disclosure:

This is the final stage to submit STR/SAR to Bangladesh Financial Intelligence Unit (BFIU), when there is valid reason/s to treat any transaction as suspicious, on the ground of ML/TF. For simplification a flow chart is given below to show STR/SAR identification and reporting procedures:



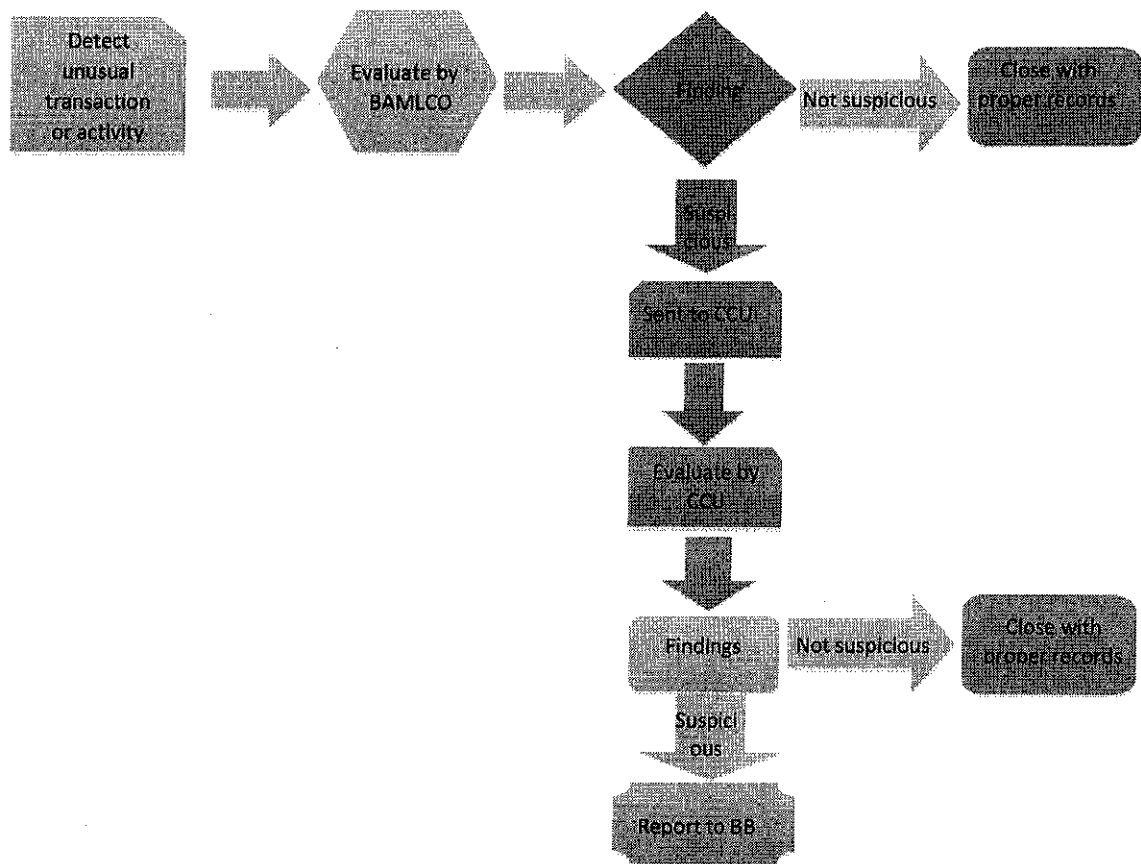


Figure: STR/SAR Reporting Process

10.6 Reporting of STR/SAR

SFIL as per Money Laundering Prevention (Amendment) Act, 2015 and Anti-Terrorism (Amendment) Act, 2013 are obligated to submit STR/SAR to Bangladesh Financial Intelligence Unit (BFIU). Such report must come to the Bangladesh Financial Intelligence Unit (BFIU) from CCU. This report must be sent to the BFIU by using GoAML.

10.7 Tipping off

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

Section 6 of Money Laundering Prevention (Amendment) Act, 2015 and FATF Recommendation no. 21



prohibits reporting agencies, their directors, officers and employees from disclosing the fact that an STR/SAR or related information is being reported to Bangladesh Financial Intelligence Unit (BFIU). A risk exists that customers could be unintentionally tipped off when SFIL is seeking to perform its CDD obligation.

10.8 Penalties of tipping off

As per section 6(2) & (3) of Money Laundering Prevention (Amendment) Act, 2015, the following penalties and/or punishment shall impose against any of the directors, officers and employees:

Section 6(2) of this Act: Any person, institution or agent empowered under this Act shall refrain from using or divulging 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.

Section 6(3) of this Act: Any person who contravenes the provisions of sub-sections (1) and (2) 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.

10.9 "Safe Harbor" provision for reporting

Safe harbor laws encourage reporting agencies 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. Section 28 of Money Laundering Prevention (Amendment) Act, 2015 provides the safe harbor for reporting agency.

10.10 Indicators of STR/SAR

10.10.1 Frequent change of customer address

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

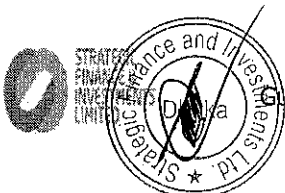
10.10.2 Out of market windfalls

Concerned officer shall pay attention to those customers/clients whose address is far from the Company, especially if there is no special reason for the same, it should be investigated whether there are institutions closer to home that could provide service to the customer. If the customer is a business man, the distance to its operations may be an attempt to prevent SFIL from verifying their business condition.

10.10.3 Suspicious customer behavior

Some typical behavior having intention to do suspicious transaction of a customer is:

- i. Unusual or excessively nervous demeanor;



- ii. Discusses on record-keeping or reporting duties with the apparent intention of avoiding them;
- iii. Threatens an employee in an effort to discourage required record keeping or reporting;
- iv. Reluctant to proceed with a transaction after being told it must be recorded;
- v. 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;
- vi. 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;
- vii. A student uncharacteristically transacts large sums of money; and
- viii. An agent, attorney or financial advisor acts for another person without proper documentation such as a power of attorney etc.

10.10.4 Suspicious customer identification

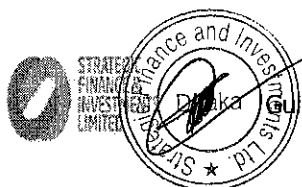
Some typical examples having intention to hide identification towards suspicious transactions of a customer:

- i. Furnishes unusual or suspicious identification documents and is unwilling to provide personal data;
- ii. Is unwilling to provide personal background information when opening an account;
- iii. Permanent address is outside the FI's service area;
- iv. Asks many questions about how the financial institution disseminates information about the identification of a customer; and
- v. Reluctant to reveal details about the business activities or to provide financial statements or documents about a related business entity.

10.10.5 Suspicious non-cash deposits

Some typical examples of non-cash deposits having intention to do suspicious transactions of a customer:

- i. Deposits large numbers of consecutively numbered money orders or round figure amounts;
- ii. Deposits cheques and/or money orders that are not consistent with the intent of the account or nature of business;
- iii. Funds out of the accounts are not consistent with normal business or personal items of the account holder; and
- iv. Funds deposited are moved quickly out of the account via payment methods inconsistent with the purpose of the account.



10.10.6 Suspicious activity in credit transactions

Some typical examples of credit transactions having intention to do suspicious transactions of a customer:

- i. Financial statement do not conform with the accounting principles;
- ii. Suddenly pays off a large problem loan with no reasonable explanation of source of funds; and
- iii. Produce/lien certificate of deposit and use as collateral of a loan/lease.

10.10.7 Suspicious commercial account activity

Some typical examples of commercial account activity having intention to do suspicious transactions of a customer:

- i. Business customer presents financial statements noticeably different from those of similar businesses; and
- ii. Large business presents financial statements that are not prepared by professional accountant.

10.10.8 Suspicious employee activity

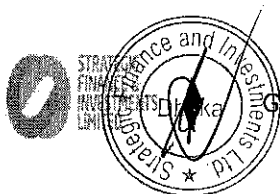
Some typical examples of activities having intention to help customer to do suspicious transactions towards ML/TF of an employee:

- i. Exaggerates the credentials, background or financial ability and resources of a customer in written reports as per Company requirements;
- ii. Frequently is involved in unresolved exceptions or recurring exceptions on exception reports;
- iii. Lives a lavish lifestyle that could not be supported by his/her salary and background; and
- iv. Frequently overrides internal controls or CCU approval authority or avoid policy.

10.10.9 Suspicious activity in an FI setting

Some typical examples of activity of a customer in relation to suspicious transactions towards ML/TF using setting of financial institution:

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



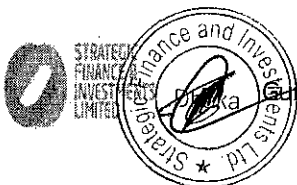
Chapter 11 : Reporting cash transaction report (CTR)

The Deputy Chief Anti-Money Laundering Compliance Officer (DCAMLCO) and Branch Anti-Money Laundering Compliance Officer (BAMLCO) will monitor and analyze the daily cash transactions and prepare Cash Transaction Report (CTR) as prescribed in the Master Circular#12, dated: June 29, 2015 of Bangladesh Financial Intelligence Unit (BFIU) under Clause#6. As per the circular:

1. In case of cash deposit or cash withdrawal and online cash deposit or any other online deposit or withdrawal in a particular account in a particular day, the transaction amount is Tk.10.00 lac and more through one or more transactions in a single/individual account, concerned officer will send a report to Central Compliance Unit (CCU) in Head Office by the end of the 2nd week of subsequent month for onward submission of the same to BFIU within 21st day of the corresponding next month using goAML web of BFIU;
2. The DCAMLCO/BAMLCO will analyze the CTR(s) meticulously before reporting the same to CCU to identify any suspicious transaction or activity. If something is found suspicious or unusual they will send them to CCU members for scrutiny and upward reporting as STR. If the CCU, after review, discovers any transaction/s as suspicious/unusual they shall direct to the responsible officer to report the account/s as STR using goAML web;
3. In case, if they don't find anything suspicious/unusual the CAMLCO will make a certification with the CTR report stating that "we have checked and didn't find anything suspicious in the CTR" and will send the same to BFIU through the Message Board of the goAML web;
4. The Head Office as well branch/es will preserve the CTR report, if any, on monthly basis;
5. The Head Office as well branch/es will keep record of the CTR at least for 5 (five) years from the date of the reporting;
6. In case of cash deposits of Government (including ministry and division) account, Government owned Organization, Semi-Government or Autonomous Organization CTR report is not applicable but in case of withdrawal the same shall be applicable; and
7. The CTR report is effective from July, 2015.
8. In case of accounts of Government, Semi Government and autonomous organizations only Cash withdrawal will be reported

The above master circular is available in link below:

<https://www.bb.org.bd/mediaroom/circulars/aml/jun292015bfui12.pdf>



Chapter 12 : Record keeping

12.1 Statutory requirement

SFIL should preserve all necessary records on transactions for a specific period as mentioned in the Companies Act, 1994.

However, in terms of section 25(1)(b) of Money Laundering Prevention (Amendment) Act, 2015, and FATF Recommendation no.11, SFIL requires to preserve previous records of transactions of closed account (s) for at least 5 (five) years from the date of closure. This will enable SFIL to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity.

Records relating to verification of identity generally comprise the followings:

- i. A description of the nature of all the evidence received relating to the identity of the verification subject; and
- ii. 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 generally comprise the followings:

- i. Details of personal identity, including the names and addresses, etc. pertaining to:
 - a. The customer;
 - b. The beneficial owner of the account or product;
 - c. The non-account holder conducting any significant one-off transaction; and
 - d. Any counter-party.
- ii. Details of transaction including:
 - a. Nature of transactions;
 - b. Volume of transactions, customer's instruction(s) and authority;
 - c. Source/s of funds;
 - d. Destination/s of funds;
 - e. Book entries;
 - f. Date of the transaction;
 - g. Form in which funds are offered and paid out;
 - h. Parties to the transaction; and
 - i. Identity of the person who conducted the transaction on behalf of the customer.

As per the Money Laundering Prevention (Amendment) Act, 2015, the records of identities of customers shall have to be kept for at least 5 (five) years from the date when the relationship with the customer has ceased. This is the date of:



- a. Closing of an account; or
- b. Providing of any financial services; or
- c. Carrying out of the one-off transaction; or
- d. Ending of the business relationship; or
- e. Commencement of proceedings to recover debts payable on insolvency.

12.2 Retrieval of records

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

12.3 STR /SAR/CTR and investigation records

SFIL should not destroy any STR/SAR/CTR related records of customer or transaction without the consent of the Bangladesh Financial Intelligence Unit (BFIU) where: (1) Company has submitted a report of suspicious transaction; or (2) it is known that a customer or any transaction is under investigation, even after expiration of the maximum preservation period of 12 (twelve) years as per law or conclusion of the case, as the case may be. To ensure the preservation of such records SFIL should maintain a register or tabular records of all investigations and inspection made by the investigating authority or BFIU and all disclosures to the BFIU. The register should be kept separate from other records and contain as a minimum the following details:

- i. The date of submission and reference of the STR/SAR/CTR;
- ii. The date and nature of the enquiry;
- iii. The authority who made the enquiry, investigation with reference; and
- iv. Details of the account(s) involved.

12.4 Training records

SFIL shall maintain training records which include:

- i. Details of the content of the training programs provided;
- ii. The names of staff who have received the training;
- iii. The date/duration of training;
- iv. The results of any testing carried out to measure staffs understanding of the requirements; and
- v. An on-going training plan.

12.5 Branch level record keeping

To ensure the effective monitoring and demonstrate compliance with the concerned regulations, SFIL shall have to ensure the keeping or availability of the following records at the Head Office and/or branch



level either in hard form or electronic form:

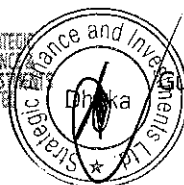
- i. Information regarding Identification of the customer;
- ii. KYC information of a customer;
- iii. Transaction report;
- iv. STR/SAR/CTR generated from the Head Office/branch;
- v. Exception report;
- vi. Training record; and
- vii. Return submitted or information provided to the Head Office or competent authority.

12.6 Sharing of record/information

Financial Institutions shall share account related information only to the investigating agency as mentioned in the para 2 (tha) of the Money Laundering Prevention (Amendment) Act, 2015.



STRATEGIC
FINANCE
INVESTMENTS
LIMITED



Chapter 13 : Non face to face customer

13.1 Definition

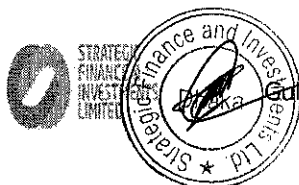
Non-face-to-face account opening refers to a situation where the customer is not interviewed and the signing of account opening forms and identification of documents of the customer are not conducted in the presence of concerned officer of a financial institution.

13.2 What to do in case of non-face-to-face customer

Sometimes, SFIL is required to open accounts on behalf of customers who do not present themselves for personal interview i.e. no face-to-face contact with the customer. In such situation collection of photographic and other related documents will not be an appropriate procedure. The following steps need to be taken under such circumstances:

- i. Apply Enhanced Due Diligence (EDD) or Enhanced Customer Due Diligence (Enhanced CDD);
- ii. Apply extensive customer identification procedures for non-face-to-face customers;
- iii. Shall not allow non-face-to-face contact to a resident in establishing relationship;
- iv. Original current passport or ID card shall be verified and certified true copy thereon shall be obtained and preserved;
- v. Ensure that there are sufficient evidences to conform address and personal identity. The concerned employee shall take at least one additional check to safeguard against impersonation;
- vi. Ask additional documents to complement those which are required for face-to-face customers;
- vii. Independent contact with such customer;
- viii. Third party introduction, where necessary;
- ix. Update customer's information more frequently than face-to-face customers; and
- x. In extreme cases, refusal of business relationship for high risk customers with the approval of the Managing Director & CEO.

The above should apply to all new as well as existing customers on the basis of materiality and risk, and accordingly due diligence should be conducted on the existing customers based on appropriate judgment.



Chapter 14 : Statement of Compliance

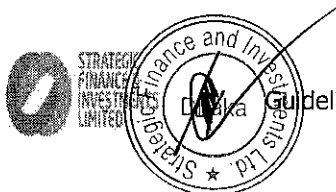
SFIL should obtain a "Statement of Compliance" on prevention of money laundering and combating terrorist financing from its all employees. Such statement should be duly signed by respective employee and preserved in the employees' personal files.

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

- i. Have read the Company's Guidelines on "Prevention of Money Laundering and Combating Terrorist Financing"; as well as circulars/directives of Bangladesh Financial Intelligence Unit (BFIU) and Government's Acts on Anti-Money Laundering and Anti-Terrorism and understood the implications thereof;
- ii. Shall comply the applicable laws and regulations and corporate ethical standards;
- iii. Shall comply all the rules and regulations in the normal course of my assignments. It is my responsibility to become familiar with the rules and regulations that relate to my assignment; and
- iv. Shall be held responsible for carrying out compliance responsibilities on prevention of Money Laundering and combating Terrorist Financing meticulously.

The CAMLCO should also ensure that all new employees of the Company shall read this policy, understand the implications there of and sign the "Statement of Compliance". After signing off, it should be sent to HR for preserving in the newly appointed employee's personal file.

A typical format on "Statement of Compliance" has been given at "**Annexure-I**" of this Guidelines.



Chapter 15 : Confidentiality of Information

All information generated, exchanged or provided with any personnel of the Company in the context of ML/TF must be on strict controls and safeguards to ensure that the information is used only in an authorized manner, consistent with provisions of regulation of the Government and Bangladesh Financial Intelligence Unit (BFIU).

15.1 Restriction on sharing of record/information as per Money Laundering Prevention (Amendment) Act, 2015 and Anti-Terrorism (Amendment) Act, 2013

- i. Any person, institution or agent empowered under these Acts shall refrain from using or divulging 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 these Acts.
- ii. Financial Institutions shall share account related information only to the investigating agency as mentioned in the para of the Money Laundering Prevention (Amendment) Act, 2015. As per para ২(ঠ) of the Money Laundering Prevention (Amendment) Act, 2015 "Investigating Agency" means-

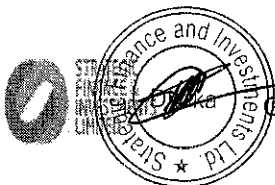
তদন্তকারী সংস্থা অর্থ এই আইনের অন্য কোন বিধানে ভিন্নরূপ কোন কিছু না থাকলে;-

(অ) দফা (শ) এ বর্ণিত "সম্পূর্ণ অপরাধ" তদন্তের জন্য সংশ্লিষ্ট আইনে ক্ষমতাপ্রাপ্ত তদন্তকারী সংস্থা; তবে শর্ত থাকে যে, যে সকল সম্পূর্ণ অপরাধ বাংলাদেশ পুলিশ কর্তৃক তদন্তযোগ্য তাহা বাংলাদেশ পুলিশের অপরাধ তদন্তযোগ্য তাহা বাংলাদেশ পুলিশের অপরাধ তদন্ত বিভাগ (criminal investigation department) কর্তৃক তদন্ত করিতে হইবে;

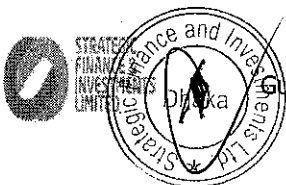
(আ) সরকারের সহিত পরামর্শক্রমে বাংলাদেশ ফাইন্যান্সিয়াল ইন্টেলিজেন্স ইউনিট কর্তৃক ক্ষমতাপ্রাপ্ত উপ-দফা (অ) এ উল্লিখিত এক বা একাধিক তদন্তকারী সংস্থা।

15.2 Penalties for disclosing information

Section 6 of Money Laundering Prevention (Amendment) Act, 2015: If any person, institution or agent empowered under this act discloses 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 purpose 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.



Part-II : Combating the Financing of Terrorism



1. Introduction

Terrorist Financing has become a massive threat in recent years. As such, terrorist financing has become a great concern for all countries in the world. It is widely acknowledged to be an essential component of terrorist activity as terrorists are able to facilitate their activities only, if they have the financial resources to do so. The consequences of terrorist activities are tremendous and devastating. So, combating financing of terrorism is indispensable for the economy and also for the security of our country. The Government of Bangladesh has given top most priority to this issue. As such, Anti-Terrorism (Amendment) Act, 2013 was enacted by the Parliament of the People's Republic of Bangladesh, which has already been amended in 2012 and 2013. The Act has been effective from the June 11, 2008. In the Anti-Terrorism (Amendment) Act, 2013 terrorist financing has been termed as criminal activity and the role of Financial Institutions (FIs) to fight against financing of terrorism has been specified. It is considered that the fight against financing of terrorism is a combined effort and policy has been drawn accordingly.

2. What is terrorist financing

As per Section 7 of Anti-Terrorism (Amendment) Act, 2013:

- i. If any person or entity willfully provides, receives, collects or makes arrangements for money, service or any other property, whether from legitimate or illegitimate source, by any means, directly or indirectly, with the intention that, it would, in full or in part, be used-
 - a) To carry out terrorist activity;
 - b) By a terrorist person or entity for any purpose, or is in the knowledge that it may be used by a terrorist person or entity; the said person or entity shall be deemed to have committed the offence of terrorist financing.
- ii. Conviction for terrorist financing shall not depend on any requirement that the fund, service or any other property mentioned in sub-section (1) was actually used to carry out or direct or attempt to carry out a terrorist act or be linked to a specific terrorist act.
- iii. If any person is convicted of any of the offences mentioned in sub-section (1), the person shall be punished with rigorous imprisonment for a term not exceeding 20(twenty) years but not less than 4(four) years, and in addition to that, a fine equivalent to twice the value of the property involved with the offence or Taka 10(ten) lac, whichever is greater, may be imposed.
- iv. If any entity is convicted of any of the offences mentioned in the sub-section (1)-
 - a) Steps may be taken against the entity in accordance with section 18 and in addition to that a fine equivalent to thrice the value of the property involved with the offence or of Taka 50(fifty) lac, whichever is greater, may be imposed; and
 - b) The head of that entity, whether he is designated a Chairman, Managing Director & CEO or by whatever name called, shall be punished with rigorous imprisonment for a term no exceeding 20 (twenty) years but not less than 4 (four) years and, in addition to that, a fine equivalent to twice the value of the property involved with the offence or of Taka 20 (twenty) lac, whichever is greater, may be imposed unless he is able to prove that the said offence was committed without his knowledge or he had tried his best to prevent the commission of the said offence.



3. International requirement on combating TF and proliferation of weapons of mass destruction

United Nations Security Council Resolution (UNSCR) 1267 and 1373 have been adopted under Article VII of UNSCR charter, which means these resolutions are obligatory for every jurisdiction. Accordingly, BFIU instructed FIs to take necessary action on UNSCR 1267 and 1373; banned list of Bangladesh Government by their circular:

- i. Introduce a Board approved policy regarding prevention of financing of terrorism and proliferation of weapons of mass destruction;
- ii. Instruct all concerned employees about their responsibilities and review the instruction, when necessary;
- iii. Introduce a software to keep records of updated lists of terrorists of UNSCR 1267 and 1373 or of Bangladesh government;
- iv. Monitor regularly the terrorists list of UNSCR or of Bangladesh Government to monitor whether any account, directly or indirectly, maintaining with SFIL. If so, shall require to be reported directly to Bangladesh Financial Intelligence Unit (BFIU) without delay; and
- v. Stop transaction of account of any person or entity whose names are listed with UNSCER 1373 and banned list of Bangladesh Government and inform BFIU immediately.

In a nut shell, to comply with this direction SFIL should require to monitor the UN sanction list and Bangladesh Government's banned list against ML/TF regularly and if any account or transaction is found to have any connection with the lists, shall have to inform BFIU immediately.

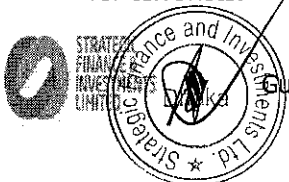
4. The link between ML and TF

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.

5. Why SFIL must combat financing of terrorism

- i. Financing of Terrorism was termed as criminal activity under United Nations International Convention for the Suppression of the Financing of Terrorism in 1999. To reinforce the 1999 Convention, United Nations adopted UNSC Resolutions 1373 and 1390 directing member states to criminalize Financing of Terrorism and adopt regulatory measures to detect, deter and freeze terrorists' assets. The resolutions oblige all countries to deny financing, support and safe harbor for terrorists.



- ii. Bangladesh has been actively involved in multinational and international institutions. Its international relationship and business, banking business in particular are regulated by some domestic and international regulations. So it is mandatory to abide by those regulations. Financial Action Task Force (FATF), the international standard setter, adopted 40 recommendations for AML/CFT in the year, 2012. So, SFIL must be involved in international effort to CFT.
- iii. It is increasingly evident that terrorists and their organizations need to raise significant amounts of cash for a wide variety of purposes for recruitment, training, travel and materials as well as often payment for safe heaven protection. So to root out terrorism, SFIL must stop the flow of funds.
- iv. The consequences of allowing the financial system to facilitate the movement of terrorist money are so terrible that every effort must be made to prevent this from happening. So CFT is not only the regulatory requirement but also an act of self-interest.

6. Purpose of the policy

Both ML and TF have been identified as major threats to the financial services community. The management of SFIL has recognized prevention of ML and combating TF as a team effort. This section outlines policies, procedures and measures to be taken for combating financing of terrorism.

7. Policy statement

Pursuant to the Money Laundering Prevention (Amendment) Act, 2015 and Anti-Terrorism (Amendment) Act, 2013, the Bangladesh Financial Intelligence Unit (BFIU) has issued a master circular #12, dated June 29, 2015 elaborating the responsibilities of FIs to prevent ML/ combat TF.

As such, SFIL is committed to implement the provisions of the Anti-Terrorism (Amendment) Act, 2013, and also the guidelines and instructions issued by BFIU from time to time in respect of transaction monitoring systems and operational processes.

SFIL is committed to assist and co-operate with the relevant law enforcement authorities, the BFIU whenever possible and to the fullest extent possible as per sub section 3 of section 15 of Anti-Terrorism (Amendment) Act, 2013.

It is the policy of SFIL to adhere to all of the provisions of Anti-Terrorism (Amendment) Act, 2013 and other regulations by implementing this policy and subsequent procedures.

8. Enforcement

Management of SFIL is responsible for ensuring that the directives are implemented and administered in compliance with the approved policy. Changes to the policy will require approval by the Board of Directors. The Management of SFIL is empowered to effect changes in operating procedures, standards, guidelines and technologies etc.

9. Exceptions to the policy

Requests for exceptions to this policy must be specific and may only be granted on specific items, rather than to entire sections. Concerned executives shall communicate their requests with exceptions to the Managing Director & CEO.



10. Procedure

All financial institutions must be committed to combat TF. Guidelines on Prevention of Money Laundering are written in **Part-I** of the guidelines.

SFIL believes that strict adherence to the existing AML Policy Guidelines provides basic AML controls which also serves as primary controls for detection and combating of TF. Therefore, in addition to the existing AML Policy Guidelines, the following extra due diligence and vigilance will be exercised to detect and combat TF.

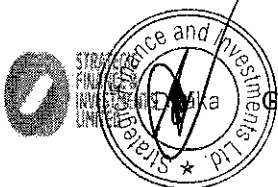
Under direct control of the Managing Director & CEO of SFIL, AMD/DMD/SEVP/EVP and all Head of Divisions on their part, Central Compliance Unit for Prevention of Money Laundering and Combating Terrorist Financing headed by CAMLCO, DCAMLCO, all Branch Manager/s, Branch Anti-Money Laundering Compliance Officers (BAMLCO), compliance officers and all other employees including contracted and outsourced staffs will be responsible for ensuring compliance with the Money Laundering Prevention (Amendment) Act, 2015 and the Anti-Terrorism (Amendment) Act, 2013 and relevant directives/circulars of Bangladesh Financial Intelligence Unit (BFIU) in this regard.

11. General procedures for Customer Due Diligence (CDD)/Know Your Customer (KYC)

- i. The new uniform account opening form and KYC profile have now become the integral part of establishing account relationship. They are mandatory and a vital reference point to all account relationship.
- ii. With regard to KYC/CDD, customer's risk assessment, record keeping and suspicious transaction reporting, concerned employees will follow the procedure as stated in the AML/CFT Guidelines.
- iii. As KYC/CDD is an important component of the AML/CFT process, the ongoing monitoring of individual transactions on customer accounts is crucial to improve the ability of the institution to detect criminal activities.
- iv. IT Division may develop automated systems and processes for classifying customers on the basis of the risk matrix provided by BFIU under new KYC Profile, monitoring transactions with the transaction profile provided by the customers & incorporating watch list as per UN Resolutions in software. These new systems will improve ability of the employees to detect unusual transactions, help the authorities to identify and respond to new money laundering and terrorist financing techniques.
- v. DCAMLCO/Branch Manager/BAMLCO/Compliance Officer, as the case may be, will monitor customer's transaction regularly in order to identify suspicious transactions/activities related to both money laundering and terrorist financing. They will also oversee the day to day activities of the Branch and confirm compliance of the instructions of concerned authority.

12. Non-profit & NGO sector

Accounts of charities, NPOs, NGOs to be treated as high risk accounts and EDD will be performed at the time of opening and operating such accounts for combating TF.



13. Training and awareness of the employees

SFIL will continue to devote considerable resource to establish and maintain employees' awareness of the risks of TF, and their competence to identify and report relevant suspicions in this area. The company is dedicated to a continuous program of increasing awareness and training of employees' at all appropriate levels in relation to their knowledge and understanding of CFT issues, their respective responsibilities and the various controls and procedures introduced by SFIL to combat TF.

14. Self-assessment

This policy requires that appropriate and timely self-assessments, tests, audits and evaluations be conducted to ensure that SFIL is in compliance with the CFT regulations. Each and every Branch shall assess their performance half yearly according to Master Circular no. 12, dated: June 29, 2015 of Bangladesh Financial Intelligence Unit (BFIU). The shortcomings identified be overcome and complied within next quarter.

15. Independent testing procedures

As per Master Circular No.12, dated: June 29, 2015, of Bangladesh Financial Intelligence Unit (BFIU) testing on CFT is to be conducted by the ICC department. While conducting the same, they should also look into, whether the directives of Anti-Terrorism (Amendment) Act, 2013; and BFIU's directives issued from time to time in this respect are followed meticulously by the Branches.

Mentionable that Compliance of CFT is the responsibility of each employee of SFIL. Therefore, all guidelines related to AML/CFT be updated as and when required and circulated and ensured that all employees are aware of the Anti-Terrorism (Amendment) Act, 2013, internal guidelines and other policies and procedures.

16. Monitoring

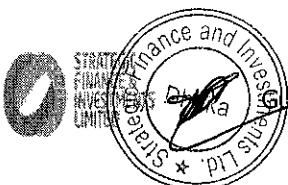
SFIL shall effectively reciprocate monitoring of procedures and controls that meet the requirements of SFIL's policy, standards and Rules and Regulations under Anti-Terrorism (Amendment) Act, 2013.

➤ Monitoring process

Appropriate monitoring program for the activities and transactions routed through the customer's account should be instituted. Depending on the type and nature of the account, SFIL may fix/set specific threshold to identify the customer activities that do not appear to commensurate with the customer's business activities.

➤ Suspicious transaction/activity report (STR/SAR):

When there is a suspicion that funds are linked to terrorist financing, concerned officer will submit identified suspicious transaction/activity to their respective DCAMLCO, BAMLCO and Compliance Officer. They shall send a copy of the same with comments through the Branch Manager to CAMLCO without any delay. The STRs/SARs must be reported to Bangladesh Financial Intelligence Unit (BFIU) within shortest possible time after due verification through CCU. Utmost secrecy must be maintained while submitting STRs/SARs as per directives of BFIU. Internal reporting format has been given in the



AML/CFT guidelines as "Annexure-H" for reporting to BFIU.

17. Responsibilities

The management of SFIL shall take necessary measures, with appropriate caution and responsibility, to prevent and identify financial transactions which are connected to any offence under the Anti-Terrorism (Amendment) Act, 2013 and shall report identified suspicious transaction/activity, if any, to Bangladesh Financial Intelligence Unit (BFIU) immediately.

The Board of Directors, or in the absence of the Board of Directors, the Managing Director & CEO shall approve and issue directions regarding the duties of its officers, and shall ascertain whether the directives issued by BFIU under section 15 of Anti-Terrorism (Amendment) Act, 2013, which are applicable to SFIL as reporting agency, have been complied or not.

The responsibilities of the officials of SFIL are presented below in tabular form for easy understanding and smooth implementation by the concerned employee/s:

| Responsible Dept. Or Officials | Responsibilities |
|--|---|
| Officer in charge who is responsible for opening new accounts/making transaction | <ul style="list-style-type: none"> a. To interview the potential customer; b. Verify customer profile; c. To arrive at threshold limit for each account (new as well as existing) and to exercise due diligence in identifying suspicious transactions/activities; d. To restrict opening of accounts in the name of terrorist/banned organizations; e. To adhere with the provisions of Money Laundering Prevention (Amendment) Act, 2015; and f. To comply with the guidelines issued by Bangladesh Financial Intelligence Unit (BFIU) and by the company from time to time in respect of opening and conduct of account. |
| Chief Risk Officer | To assess the ML risk involves in operating activities of the Company and to evaluate adequacy and effectiveness of the control mechanism set for safeguarding the company's risks. |
| Head of Operations | <ul style="list-style-type: none"> a. To scrutinize and ensure that the information furnished in the account opening form/customer profile/threshold limit are in strict compliance with AML/CFT Guidelines before authorizing opening of account; and b. To certify regarding compliance with AML/CFT Guidelines and report suspicious transactions to CAMLCO/Managing Director & CEO. |
| Internal Auditor | To verify and record his comments on the effectiveness of measures taken by the concerned officials and the level of implementation AML/CFT Guidelines. |
| CAMLCO | <ul style="list-style-type: none"> a. To implement and enforce Company's AML policies; b. To ensure sending STR/SAR/CTR to BFIU; c. To inform DCAMLCO/BAMLCO required actions, if any, to be taken. |



| | |
|-------------------------|---|
| DCAMLCO | <ul style="list-style-type: none"> a. To assist CAMLCO to implement and enforce Company's AML policies; b. Send STR/SAR/CTR to BFIU through CCU; c. Ensuring flow of information to BAMLCO towards reporting to CAMLCO and CCU; and |
| BAMLCO | <ul style="list-style-type: none"> a. Ongoing monitoring of customer's KYC profile/CDD/EDD and transaction activities; b. Report STR/SAR/CTR through branch manager to CAMLCO and CCU; c. Provide AML training to branch employees; d. Communicate and update to all employees in case of any changes in national or Company's own policies; e. Organize a meeting with all executives/officers at least once after each quarter end as per Master Circular#12/2015 of Bangladesh Financial Intelligence Unit (BFIU); and f. Submit Self-Assessment Report to CAMLCO/CCU/ICC. |
| Branch Manager | <ul style="list-style-type: none"> a. Ensure that the AML program is effective within the Branch; b. Overall responsibility to ensure that the Branch has an effective AML program in place and that it is working effectively. |
| Top Management | Prompt reporting of information regarding suspicious transactions to concerned law enforcing authority in consultation with the competent authority/ies. |
| Managing Director & CEO | Overall responsibility to ensure that SFIL has AML program in place and that it is working effectively. |

However appropriate disciplinary action will be initiated against the delinquent official for violation of this policy.

18. Customer acceptance policy

Pursuant to the above legal bindings, Guidance Notes issued by Bangladesh Financial Intelligence Unit (BFIU) on AML/CFT and Global standards, SFIL has developed the Customer Acceptance Policy stated at "Annexure-B".

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

- a) According to section 16(3), if any reporting agency fails to comply with the directions laid down in section 16(1), the said reporting agency shall be liable to pay a fine determined and directed by Bangladesh Financial Intelligence Unit (BFIU) not exceeding Taka 25 (twenty five) lac and BFIU may suspend the registration or license of the organization or any of its branches, service centers, booths or agents for the purpose of closing its operation within Bangladesh, or shall inform the registration or licensing authority about the fact so that the relevant authority may take appropriate measures against the said organization.
- b) According to section 16(4), if the Board of Directors, or in the absence of the Board of Directors (BoD), Managing Director & CEO, by whatever name called, of any reporting agency fails to comply with the directions laid down in section 16(2), the Chairman of the Board of Directors, or the Managing Director & CEO in relevant cases shall be liable to pay a fine not exceeding Taka 25



(twenty five) lakh and BFIU can terminate the person from the position or in relevant cases shall inform the relevant authority about the issue to take proper steps against him/her.

- c) According to section 16(5), if any reporting agency fails to pay or does not pay any fine imposed by BFIU under section 16(3), or if the Chairman of the Board of Directors, or the Managing Director & CEO, fails to pay or does not pay any fine imposed by BFIU under section 16(4), BB may recover the amount from the reporting agency or by debiting its account maintained in any bank or FI or BB and if any amount of fine remains unrealized or unpaid, BFIU may, if necessary, make an application to the concerned court for recovery.

20. Schedule of Anti-Terrorism (Amendment) Act, 2013

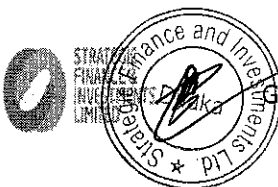
Three schedules have been annexed at the end of this ATA Policy as "Schedule-1", "Schedule-2" and "Schedule-3" as prescribed in the Anti-Terrorism (Amendment) Act, 2013 and accordingly SFIL shall pursue those for combating TF.



"Schedule-1"

[See clause (3A) of section 2 of Anti-Terrorism (Amendment) Act, 2013]

- a) Convention for the suppression of unlawful seizure of Aircraft done at the Hague on 16th December, 1970;
- b) Convention for the suppression of unlawful acts against the safety of Civil aviation, done at Montreal on 23rd September, 1971;
- c) Convention on the prevention and punishment of Crimes against internationally protected person, including diplomatic agents, adopted by the General Assembly of the United Nations on 14th December, 1973;
- d) International convention against the taking of hostages adopted by the General Assembly of the United Nations on 17th December, 1979;
- e) Convention on the physical protection of nuclear material, adopted at Vienna on 3rd March, 1980;
- f) Protocol for the suppression of unlawful acts of violence at airports serving International Civil Aviation, supplementary to the convention for the suppression of unlawful acts against the safety of Civil Aviation, done at Montreal on 24th February, 1988;
- g) Convention for the suppression of unlawful acts against the safety of maritime navigation, done at Rome on 10th March, 1988;
- h) Protocol for the suppression of unlawful acts against the safety of fixed platforms located on the continental shelf, done at Rome on 10th March, 1988;
- i) International convention for the suppression of terrorist bombings, adopted by the General Assembly of the United Nations on 15th December, 1997.



"Schedule-2"

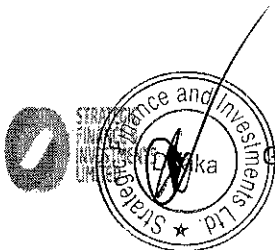
[See section 18 of Anti-Terrorism (Amendment) Act, 2013 and Circulars issued by BFIU from time to time]

| Serial No. | Name of the entities | Date of Proscription | Address of the entity | Remarks |
|------------|---|----------------------|--|---------|
| 01 | Shahadat-e-al-Hikma Party Bangladesh | 09/02/2003 | Mizanur Rahman's Home, Harogram Notun Para Bypass Road, P.S.Rajpara, Rajshahi Mahanagor. | |
| 02 | Jagroto Muslim Janata Bangladesh (JMB) | 23/02/2005 | No Specific Address Available | |
| 03 | Jamatul Mujahidin | 23/02/2005 | No Specific Address Available | |
| 04 | Harkat-ul-Jihad al-Islami | 17/10/2005 | No Specific Address Available | |
| 05 | Hizbut Tahrir Bangladesh | 22/10/2009 | H.M. Siddique Mansion, 55/A Old Paltan, Dhaka; 201/C Paltan tower (2nd Floor), 27 Old Paltan Lane, Dhaka | |
| 06 | Ansarullah Bangla Team | 22/05/2015 | No Specific Address Available | |
| 07 | Ansar-Al-Islam | 12/04/2017 | No Specific Address Available | |
| 08 | 'Allahr Dal' alias 'Allah-er- Dol' alias 'Allahr Dol' | 04/03/2020 | No Specific Address Available | |

"Schedule-3"

[See section 18 of Anti-Terrorism (Amendment) Act, 2013]

| Serial No. | Name of the entities | Date of Proscription | Address of the entity | Remarks |
|------------|----------------------|----------------------|-----------------------|---------|
| | | | | |
| | | | | |
| | | | | |
| | | | | |



"Annexure-A"

Bond of Transparency



A/c Name:.....
Address:.....

Subject: Greetings from Strategic Finance & Investments Limited (SFIL)

Dear Sir/Madam,

We thank you for opening/maintaining account/s with Strategic Finance & Investments Limited (SFIL). We assure you our best professional service with utmost care all the time. Please check the following information as it appears in our record:

| | | |
|-------------------------|---|--|
| Product/service name | : | |
| Agreement/TDR No. | : | |
| Rate of interest | : | |
| Sanction/deposit amount | : | |
| Tenure | : | |

Kindly confirm the above information within 15(fifteen) days after receiving the letter at your end by mailing the sub-join portion. In case of non-receipt of any objection within said 15(fifteen) days of the letter, the above information will be deemed to have been confirmed.

An addressed envelope along with required stamps is enclosed for your reply. We are looking forward a warm lasting relationship with you.

Thanking you,

Yours truly,

Authorized Signature

Managing Director & CEO
Strategic Finance & Investments Limited (SFIL)
Rangs RL square, Level: 3, 201/1 Kha, Progoti Shoroni,
Dhaka-1212.

Date:

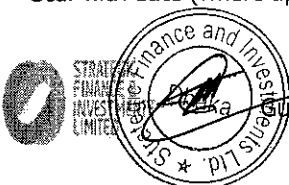
Subject: Acknowledgement

I/we hereby acknowledged and confirmed the correctness of the information mentioned in your letter ref no#....., dated: in respect of my account/agreement # opened and/or maintained with you.

Yours faithfully,

Customer's Signature:

Seal with date (where applicable):

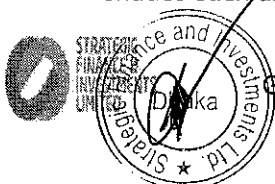


CUSTOMER ACCEPTANCE POLICY OF
STRATEGIC FINANCE & INVESTMENTS LIMITED (SFIL)

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

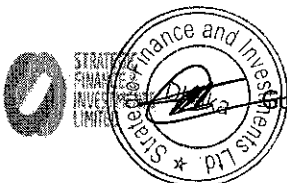
On the other hand to combat risk of Money Laundering (ML) and Financing of Terrorism (TF) Know Your Customer (KYC) and Customer Due Diligence (CDD) are important tools. Lack of precaution in the above mentioned factors might result in serious customer and counterparty risks, especially reputation, operational, legal and compliance risks. Collection of sufficient information about the customers is the most effective defense for combating ML/TF activities. As per Money Laundering Prevention Act (MLPA)-2012 (as amended in 2015) each financial institution (FI) is required to keep satisfactory evidence of the clients. On the other hand, each FI is also required to make necessary arrangement to prevent transactions related to crimes as described in Anti-Terrorism Act (ATA)-2009 (as amended in 2013). It also requires to identify, under these laws, suspicious transactions with due care and diligence. Pursuant to the above legal bindings, Guidance Notes issued by Bangladesh Financial Intelligence Unit (BFIU) on ML/TF and Global standards, SFIL has developed the Customer Acceptance Policy as under:

- 1) SFIL will comply all the prevailing regulations of MLPA-2012 (as amended in 2015) and ATA-2009 (as amended in 2013) and Bangladesh Financial Intelligence Unit (BFIU) Guidelines relating to establishing financial relationship with customers.
- 2) Documentation requirements and other information shall be collected in compliance with the instructions contained in BFIU Circular#02 dated July 17, 2002; the requirements of the MLPA-2012 (as amended in 2015) and ATA-2009 ((as amended in 2013) and other circulars and guidelines issued/ to be issued by Bangladesh Financial Intelligence Unit (BFIU) from time to time.
- 3) SFIL will not open or maintain any account or establish any financial relationship with person(s) or organization(s) convicted for terrorism or terrorist financing or listed on the United Nations Security Council Resolution (UNSCR) 1267 & 1373-as individual, entities, alliances - terrorist or terrorist organizations.
- 4) In case of opening account of a Politically Exposed Person (PEP), SFIL will comply the instructions contained in BFIU Circular#14 dated September 25, 2007 issued by Bangladesh Financial Intelligence Unit (BFIU). Such types of account will be classified as high risk and will require very high level of monitoring. PEPs account shall be opened with prior permission of the Managing Director and CEO.
- 5) At the time of opening new account SFIL will take care to seek only such information from the customer which is relevant but not intrusive. As customers profile and information contained therein are confidential documents, those should not be divulged for any other purposes.
- 6) SFIL will conduct necessary checks before opening a new account so as to ensure that the name of the customers do not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations etc. as declared by the Government



authorities.

- 7) SFIL will collect complete and correct information of identity of the beneficial owners and preserve in the concerned file. A person shall be treated as a beneficial owner if (i) he or she has controlling share of a company or and (ii) hold 20% or more share of a company.
- 8) SFIL will, in case a customer operate an account on behalf of another person in his/her own name, collect complete and correct information of the person besides the account holders.
- 9) SFIL will ensure certification/genuineness of the given documents/National ID/Social Security Number/Residence Permit/TIN, independent contact with the customer etc. in case of establishing business relationship with "Non-Face to Face Customer/Non-resident Bangladeshi".
- 10) SFIL will review the customer's personal/business background with due diligence before establishing any financial relationship.
- 11) SFIL, in no cases, will allow any anonymous or fictitious accounts to be opened/ to be continued.
- 12) Customers' risk shall be assessed as defined in KYC Profile meticulously and shall review the same at least once in a year or at the time of renewal or providing loan against FDR or new sanction or any other business relationship.
- 13) SFIL will accept only those customers who can provide documents relating to identity and physical existence of business or residence.
- 14) The Branches shall not open any account, where SFIL is unable to apply appropriate customer due diligence measures but the branch must be careful to avoid unnecessary harassment of the customer.
- 15) SFIL will verify identity of the customers using reliable sources, documents etc. but it must retain copies of all references, documents used to verify the identity of the customers.
- 16) SFIL will comply Uniform Account Opening Form with prescribed KYC at the time of completing account opening formalities as per BFIU Circular Letter#02 dated: March 15, 2015.
- 17) SFIL will take necessary steps to close existing accounts, where necessary, due to non-cooperation of the customers in providing necessary documents/information required by law/regulatory authority or non-reliability of the information/documents furnished by them. Decision to close an account shall be subject to approval of the Managing Director & CEO.
- 18) SFIL will not do anything that will cause inconvenience to the general public, especially those who are financially or socially disadvantaged.
- 19) SFIL, in no cases, will deal with any Shell company or Shell bank.
- 20) SFIL reserves the right to discontinue or close relationship, which in its opinion has contravened the MLPA-2012 (as amended in 2015) and ATA-2009 (as amended in 2013), and any other laws of the Country or indicates suspicious transaction/business.



RISK ASSESSMENT FORM

"Annexure-C"

CIF No. :

Name of the Depositor:

Risk category on Profession/ Business:

Account No. :

| Sl | Nature | Risk Level | Score | Sl | Nature | Risk Level | Score |
|----|---|------------|-------|----|---|------------|-------|
| 1 | Jewellery /Gold Business | High | 5 | 22 | Motor Parts Business | Medium | 3 |
| 2 | Money Changer/Courier service agent | High | 5 | 23 | Tobacco and Cigarette business | Medium | 3 |
| 3 | Real Estate Agent/ promoter of Construction Project | High | 5 | 24 | Freight/Shipping/Cargo Agents | Medium | 3 |
| 4 | Offshore Corporation | High | 5 | 25 | Auto Business (New Car) | Low | 2 |
| 5 | Art/Antique Dealer | High | 5 | 26 | Shop Owner (Retail) | Low | 2 |
| 6 | Owner of Restaurant/Bar/Night Club/ Residential Hotel | High | 5 | 27 | Land/Property broker | Low | 2 |
| 7 | Import/Export Agent | High | 5 | 28 | Provident/Gratuity Fund | Low | 2 |
| 8 | Cash Financing Business | High | 5 | 29 | Small Business | Low | 2 |
| 9 | Share/Stock Dealer | High | 5 | 30 | Self employed Professional | Low | 2 |
| 10 | Business in different places | High | 5 | 31 | Corporate Customer | Low | 2 |
| 11 | Cinema Producer/Distributor | High | 5 | 32 | Construction Material Business | Low | 2 |
| 12 | Arms Business | High | 5 | 33 | Computer/Mobile Phone Dealer | Low | 2 |
| 13 | Mobile Phone Operator | High | 5 | 34 | Software business | Low | 2 |
| 14 | Man power Export Business | High | 5 | 35 | Manufacturer (Except Arms) | Low | 1 |
| 15 | Travel Agent | High | 5 | 36 | Retired Person | Low | 1 |
| 16 | Auto Dealer (Reconditioned Car) | Medium | 5 | 37 | Service/Job | Low | 0 |
| 17 | Leasing/Finance Company/Bank | Medium | 4 | 38 | Housewife | Low | 0 |
| 18 | Carrying Operator | Medium | 3 | 39 | Student | Low | 0 |
| 19 | Insurance/Brokerage agency | Medium | 3 | 40 | Farming/ Agriculturist | Low | 0 |
| 20 | Religious organization | Medium | 3 | 41 | Others-According to type, FI will fix risk rating | | |
| 21 | Amusement Park/Organization | Medium | 3 | | | | |

Risk Categorization:

Based on net worth

| Amount in Taka | Risk Level | Risk Rating |
|---------------------------|------------|-------------|
| Up to Taka 50 Lac | Low | 0 |
| Taka 50 Lac- Taka 100 Lac | Medium | 1 |
| > Taka 100 Lac | High | 3 |

Based on type of account opening

| Type | Risk Level | Risk Rating |
|------------------------------|------------|-------------|
| Relationship Manager/Branch | Low | 0 |
| Direct Sales Agent | Medium | 1 |
| Internet/walk in/Unsolicited | High | 3 |

Overall Risk Rating

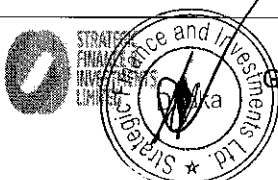
| Risk Rating | Nature of Risk |
|-------------|----------------|
| > = 8 | High |
| < 8 | Low |

Comment by BAMLCO/Head of Branch:

Overall Risk rating is in low / high level based on verification of profession and risk categorization by Relationship Manager. Also considering amount within.....lac

Date & Signature of the Dealing person

Date & Signature of BAMLCO/Branch Head



"Annexure-D"
KYC PROFILE FORM

| | | |
|-----------------------------------|--|--|
| 1. Name of the Depositor | | |
| 2. Type of Account | | |
| 3. Customer ID No. | | |
| 4. Name & Code of Dealing Officer | | |
| 5. Passport No. | | Photocopy Received? <input type="checkbox"/> Yes <input type="checkbox"/> No (if applicable) |
| 6. Birth Registration No. | | Photocopy Received? <input type="checkbox"/> Yes <input type="checkbox"/> No (if applicable) |
| 7. National Id No. | | Photocopy Received? <input type="checkbox"/> Yes <input type="checkbox"/> No (if applicable) |
| 8. eTIN No. | | Photocopy Received? <input type="checkbox"/> Yes <input type="checkbox"/> No (if applicable) |
| 9. VAT Registration No. | | Photocopy Received? <input type="checkbox"/> Yes <input type="checkbox"/> No (if applicable) |
| 10. Driving License No. | | Photocopy Received? <input type="checkbox"/> Yes <input type="checkbox"/> No (if applicable) |

11. Information of Beneficial Owner (In case of company, detail information of the controlling shareholders or shareholders holding 20% & above shares of the company)

| |
|--|
| |
|--|

12. Source of fund and how it was verified :

| |
|--|
| |
|--|

13. Details of customer's occupation with nature:

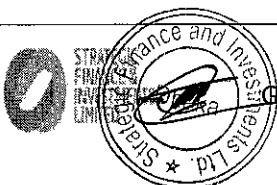
| |
|--|
| |
|--|

14. Is the amount matched with customer's income level :

| |
|--|
| |
|--|

Seal & Sign with Date

| | | |
|-------------------------------|---------------------------------------|--------|
| | | |
| Official/Relationship Manager | Team Leader/Supervisor/ Head of Dept. | BAMLCO |



KNOW YOUR EMPLOYEE (KYE) FORM

1. Personal Details:

| | | | |
|---------------------|--|-------------------|--|
| Full Name (English) | MR./ MS. | | |
| Employee Id | | Insurance Id | |
| Designation | | Department | |
| Date Of Birth | | Place Of Birth | |
| Permanent Address | | Present Address | |
| Date Of Joining | | Confirmation Date | |
| Type Of Employment | <input type="checkbox"/> PERMANENT <input type="checkbox"/> CONTRACTUAL <input type="checkbox"/> Other | | |
| Reference | | | |
| Blood Group | | Religion | |

2. Family Details:

| | |
|---------------------|--|
| Mother's Name | |
| Mother's Profession | |
| Father's Name | |
| Father's Profession | |
| Spouse Name | |
| Spouse Profession | |

3. Educational Background:

| Educational Qualification | Institutions Name | Results |
|---------------------------|-------------------|---------|
| S.S.C | | |
| H.S.C | | |
| Bachelors' | | |
| Masters' | | |
| Professional Degree | | |

4. Professional Background:

| Employer's Name | Address | Designation | Department | Contact Number | Fax Number | Release Order Received From Previous Employer |
|-----------------|---------|-------------|------------|----------------|------------|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |



5. Identification:

| | |
|--------------------------|--|
| National Id | |
| Passport Number (If Any) | |
| Tin Number (If Any) | |
| Driving License (If Any) | |

6. Contact Details

| | |
|------------------------------------|--|
| Present Address | |
| Permanent Address | |
| Phone Number (Mobile) | |
| Phone Number (Resident) | |
| Phone Number (Office) | |
| Email Address (Personal) | |
| Email Address (Office) | |
| Emergency Contact Name & Phone No. | |
| Relationship With Employee | |

7. Others

| | | | |
|--|--|---------------|--|
| Political Involvement | <input type="checkbox"/> Yes <input type="checkbox"/> No | Residing At | <input type="checkbox"/> Rented House <input type="checkbox"/> Own |
| If Rented From How Many Residence You Have Changed In Last 5 Year: | | | |
| Doing Part Time Job With Other Organization | <input type="checkbox"/> Yes <input type="checkbox"/> No | | |
| If Yes, Please Provide The Name Of The Organization And Position | | | |
| Involvement With Any Other Business | <input type="checkbox"/> Yes <input type="checkbox"/> No | | |
| If Yes, Please Provide The Name Of The Business | | | |
| Immediate Previous Residence Address | | | |
| Travel Record (Abroad) | | Owned Vehicle | <input type="checkbox"/> Yes <input type="checkbox"/> No |

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

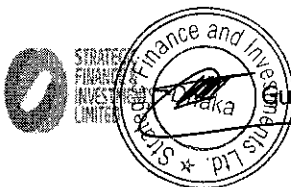
Signature of the Employee with date

To be filled up by Human Resource Department

| | |
|--|--|
| Attested Copy Of Educational Certificates Received | <input type="checkbox"/> Yes <input type="checkbox"/> No |
| Original Copy Of Educational Certificates Seen | <input type="checkbox"/> Yes <input type="checkbox"/> No |
| Police Clearance Certificate | <input type="checkbox"/> Yes <input type="checkbox"/> No |
| KYE Review Date | |

Authorized Signature
HR Department

Authorized Signature
CAMLCO



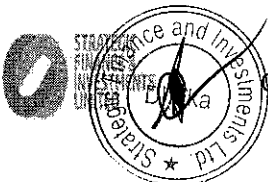
স্ট্রাটেজিক ফাইন্যান্স এন্ড ইনভেস্টমেন্টস্ লিমিটেড

প্রধান কার্যালয়, ঢাকা

শাখা কর্তৃক Self-Assessment পদ্ধতির মাধ্যমে নিজস্ব অবস্থান নির্ণয়

..... তারিখ সমাপ্ত সময়ের জন্য

| প্রশ্নমালা | যাচাইয়ের মানদণ্ড | শাখার বর্তমান-অবস্থা | গৃহীতব্য কার্যক্রম/সুপারিশ |
|--|--|----------------------|----------------------------|
| ১. শাখায় মোট কর্মকর্তার সংখ্যা কত (পদানুযায়ী)? কতজন কর্মকর্তা মানিলভারিং প্রতিরোধ বিষয়ক আনুষ্ঠানিক প্রশিক্ষণ গ্রহণ করেছেন? (শতকরা হার)? | প্রশিক্ষণ সংক্রান্ত রেকর্ড যাচাই করতে হবে। | | |
| ২. ক) শাখার মানিলভারিং প্রতিরোধ পরিপালন কর্মকর্তা (BAMLCO) জেষ্ঠ্য ও অভিজ্ঞ কিনা? বিগত দুই বছরে তিনি মানিলভারিং প্রতিরোধ ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধ বিষয়ক কোন প্রশিক্ষণ পেয়েছেন কিনা? খ) শাখায় মানি লভারিং প্রতিরোধ কার্যক্রম যথানিয়মে পরিপালিত হচ্ছে এ বিষয়টি নিশ্চিত হওয়ার লক্ষ্যে BAMLCO নির্দিষ্ট ও গ্রহণযোগ্য সময় পর পর এবং কার্যকর প্রক্রিয়ায় মনিটরিং ও পর্যালোচনা করে থাকেন কিনা? | BAMLCO কর্তৃক- KYC কার্যক্রমের যথার্থতা মনিটরিং করা হয় কিনা? যথাযথভাবে Transaction মনিটরিং এবং সন্দেহজনক লেনদেন রিপোর্ট (ইন্টারনাল রিপোর্টসহ) করা হয় কিনা? যথাযথভাবে রেকর্ড সংরক্ষণ করা হয় কিনা? STR সনাক্তকরণে ব্যবস্থা নেয়া হয় কিনা? | | |
| ৩. BAMLCO সহ শাখার কর্মকর্তাগণ মানিলভারিং ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধ বিষয়ে বিদ্যমান আইন, বিধিমালা, বিএফআইইউ কর্তৃক সময় সময় জারীকৃত নির্দেশনা ও ব্যাংকের নিজস্ব মানি লভারিং প্রতিরোধ ও সন্ত্রাসে অর্থায়ন প্রতিরোধ নীতিমালা সম্পর্কে অবহিত আছেন কি? | বিষয়টি যাচাইয়ের পদ্ধতি কি? | | |
| ৪. শাখা পর্যায়ে ত্রৈমাসিক ভিত্তিতে মানি লভারিং ও সন্ত্রাসে অর্থায়ন প্রতিরোধ বিষয়ক সভা অনুষ্ঠিত হয় কিনা? | গভার আলোচ্যসূচি সকলের অবগতির জন্য বণ্টন করা হয় কিনা? সভায় কী কী গুরুত্বপূর্ণ সিদ্ধান্ত গৃহীত হয়েছে? সভায় গৃহীত সিদ্ধান্ত কিভাবে বাস্তবায়িত হয়? | | |
| ৫. সকল প্রকার হিসাব খোলা ও লেনদেন পরিচালনার ক্ষেত্রে মানি লভারিং প্রতিরোধ আইন, সন্ত্রাস বিরোধী আইন এবং সময়ে সময়ে বিএফআইইউ কর্তৃক জারীকৃত নির্দেশনা অনুসারে গ্রাহক পরিচিতি সন্তোষজনকভাবে গ্রহণ করা হয় কিনা? | গ্রাহক পরিচিতির যথার্থতা কিভাবে যাচাই করা হয়? কিভাবে তা শাখায় সংরক্ষণ করা হচ্ছে? KYC সম্পাদনকালে গ্রাহকের তহবিলের উৎস যাচাই করা হয় কিনা? হিসাবের প্রকৃত সুবিধাভোগী (Beneficial Owner) সনাক্ত করা হয় কিনা এবং তা যাচাই এর প্রক্রিয়া সন্তোষজনক কিনা? উচ্চ ঝুঁকিবিশিষ্ট গ্রাহকদের ক্ষেত্রে ঝুঁকির নিরীখে অতিরিক্ত তথ্য (EDD) সংগ্রহ করা হয় কিনা? | | |

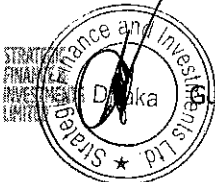


| প্রশ্নমালা | যাচাইয়ের মানদণ্ড | শাখার বর্তমান-অবস্থা | গৃহীতব্য কার্যক্রম/সুপারিশ |
|--|---|----------------------|----------------------------|
| ৬. ক) ঝুঁকির ভিত্তিতে শাখা তাদের গ্রাহকদের শ্রেণীবিন্যাস/শ্রেণীকরণ করে কিনা? | করে থাকলে এ পর্যন্ত কতটি উচ্চ ঝুঁকি সম্পন্ন হিসাব শাখায় খোলা হয়েছে? এ ধরনের হিসাব খোলা ও পরিচালনার ক্ষেত্রে শাখা কী পদক্ষেপ গ্রহণ করেছে? | | |
| ৭. বিএফআইইউ কর্তৃক জারীকৃত নির্দেশনা এবং প্রতিষ্ঠানের নিজস্ব নীতিমালা অনুযায়ী মানি লন্ডারিং ও সন্ত্রাসে অর্থায়ন সংক্রান্ত ঝুঁকি প্রতিরোধে যথাযথ ব্যবস্থা গ্রহণ করা হয়েছে কিনা? | এ বিষয়ক নিজস্ব নীতিমালা প্রণয়ন করা হয়েছে কিনা? হলে উক্ত নীতিমালা শাখায় কিভাবে বাস্তবায়িত হচ্ছে? | | |
| ৮. শাখা গ্রাহকের KYC Profile এর তথ্য বিএফআইইউ কর্তৃক জারীকৃত নির্দেশনা মোতাবেক নির্দিষ্ট সময় পর পর পুনঃমূল্যায়নপূর্বক হালনাগাদ করে কিনা? | কী পদ্ধতিতে এরূপ মূল্যায়ন সম্পাদিত হয়ে থাকে? | | |
| ৯. সন্ত্রাস বিরোধী আইন, ২০০৯ এর অধীন সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধের লক্ষ্যে শাখা কী ধরনের পদক্ষেপ গ্রহণ করেছে? | জাতিসংঘের নিরাপত্তা পরিষদের বিভিন্ন রেজুলেশনের আওতায় সন্ত্রাস, সন্ত্রাসী কার্য ও ব্যাপক ধ্বংসাত্মক অস্ত্র বিস্তারে অর্থায়নে জড়িত সন্দেহে তালিকাভুক্ত কোন ব্যক্তি বা সত্তা এবং বাংলাদেশ সরকার কর্তৃক তালিকাভুক্ত কোন ব্যক্তি বা নিষিদ্ধ ঘোষিত সত্তার নামের তালিকা শাখায় সংরক্ষণ ও তদানুসারে হিসাব ও লেনদেন কার্যক্রম যাচাই করা হয় কিনা? শাখা এ বিষয়ক নিজস্ব কোন Mechanism অনুসরণ করে কিনা? এরূপ কোন ব্যক্তি বা সত্তার নামে শাখায় পরিচালিত হিসাবের (যদি থাকে) বিষয়ে বিএফআইইউ কে অবহিত করা হয় কিনা? | | |
| ১০. এ যাবৎ শাখা কর্তৃক কতগুলো সন্দেহজনক লেনদেন (STR) শনাক্ত করা হয়েছে? | শাখায় সন্দেহজনক লেনদেন চিহ্নিত করার কোন পদ্ধতি অনুসরণ করা হয় কিনা? শাখায় সন্দেহজনক লেনদেন রিপোর্টিং এর জন্য Internal Reporting Mechanism চালু রয়েছে কিনা? শাখা পর্যায়ে নিষ্পত্তিকৃত Internal Report সংরক্ষণ করা হয় কিনা? | | |
| ১১. মানি লন্ডারিং প্রতিরোধ আইন, সন্ত্রাস বিরোধী আইন, সার্কুলার, প্রশিক্ষণ রেকর্ড, বিবরণী ও অন্যান্য AML/CFT সংক্রান্ত বিষয়বলীর আলাদা নথি শাখা কর্তৃক সংরক্ষণ করা হয় কিনা? আইন, সার্কুলার ইত্যাদির কপি শাখার সকল কর্মকর্তা/কর্মচারীদের সরবরাহ করা হয় কিনা? | সংরক্ষিত হয়ে থাকলে হ্যাঁ অথবা না হয়ে থাকলে না, আংশিক হলে কী কী সংরক্ষিত আছে তা লিখুন। | | |



| প্রশ্নমালা | যাচাইয়ের মানদণ্ড | শাখার বর্তমান-অবস্থা | গৃহীতব্য কার্যক্রম/সুপারিশ |
|--|---|----------------------|----------------------------|
| ১২. বিএফআইইউ মাস্টার সার্কুলার অনুসারে শাখায় PEPs, প্রভাবশালী ব্যক্তি, আন্তর্জাতিক সংস্থার প্রধান বা উচ্চ পর্যায়ের কর্মকর্তার কোন হিসাব সংরক্ষণ করা হচ্ছে কিনা? | উত্তর হ্যাঁ হলে এই হিসাব খোলা ও পরিচালনার ক্ষেত্রে কী কী ধরনের সতর্কতা অবলম্বন করা হচ্ছে? | | |
| ১৩. আর্থিক প্রতিষ্ঠানের প্রধান কার্যালয়, বাংলাদেশ ব্যাংক ও বাংলাদেশ ফাইন্যান্সিয়াল ইন্টেলিজেন্স ইউনিট-এর পরিদর্শন প্রতিবেদনে উল্লেখিত মানি লন্ডারিং প্রতিরোধ ও সম্ভ্রাসে অর্থায়ন প্রতিরোধ পরিপালন বিষয়ক দুর্বলতা/অনিয়মসমূহ নিয়মিত করা হয়েছে কিনা? | না হয়ে থাকলে প্রতিবন্ধকতাসমূহ কী কী? | | |

| | |
|---|--|
| শাখা মানি লন্ডারিং প্রতিরোধ পরিপালন কর্মকর্তার নামযুক্ত সীলসহ সাক্ষর ও তারিখ | শাখা ব্যবস্থাপকের নামযুক্ত সীলসহ সাক্ষর ও তারিখ |
|---|--|



অভ্যন্তরীণ নিরীক্ষা বিভাগ
স্ট্রাটেজিক ফাইন্যান্স এন্ড ইনভেস্টমেন্টস্ লিমিটেড
প্রধান কার্যালয়, ঢাকা

Independent Testing Procedures

..... শাখার পরিদর্শনের চেকলিস্ট
..... তারিখ সমাপ্ত সময়ের জন্য

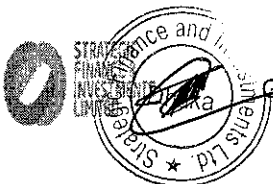
| ক্রমিক নং | অঞ্চল/এরিয়া | প্রশ্নমালা | যাচাইয়ের মানদণ্ড | স্কোর | প্রাপ্ত স্কোর | মন্তব্য | |
|--------------|--------------------------|------------|---|--|------------------|---------|--|
| ১ | শাখা পরিপালন ইউনিট | ১ | শাখায় একজন অভিজ্ঞ ও জ্যেষ্ঠ পরিপালন কর্মকর্তা (BAMLCO) রয়েছেন কি? | অফিস অভ্যন্তর দেখুন। শাখার দ্বিতীয় কর্মকর্তা বা অভিজ্ঞ কোন উর্ধ্বতন কর্মকর্তাকে BAMLCO মনোনীত করা উচিত হবে। | ১ | | |
| | | ২ | বিগত দুই বছরে তিনি মানি লন্ডারিং প্রতিরোধ ও সন্ত্রাসে অর্থায়ন প্রতিরোধ বিষয়ক কোন প্রশিক্ষণে অংশগ্রহণ করেছেন কি? মানি লন্ডারিং ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধ বিষয়ে বিদ্যমান আইন, বিধিমালা, বিএফআইইউ কর্তৃক সময় সময় জারীকৃত নির্দেশনা ও গাইডেন্স নোটস এবং প্রতিষ্ঠানের নিজস্ব মানিলন্ডারিং প্রতিরোধ ও সন্ত্রাসে অর্থায়ন প্রতিরোধ নীতিমালা সম্পর্কে তিনি যথেষ্ট অবহিত কি? | সাক্ষাৎকার ও নথিপত্রের ভিত্তিতে যাচাই করুন। | ২ | | |
| | | ৩ | মানি লন্ডারিং প্রতিরোধ আইন, সন্ত্রাস বিরোধী আইন এবং এর আওতায় জারীকৃত পলিসি এবং/অথবা নির্দেশনা যথানিয়মে পরিপালিত হচ্ছে- এ বিষয়টি নিশ্চিত হওয়ার লক্ষ্যে BAMLCO নির্দিষ্ট ও গ্রহণযোগ্য সময় পর পর এবং কার্যকর প্রক্রিয়ায় মনিটরিং ও পর্যালোচনা করে থাকেন কি? | BAMLCO কর্তৃক মনিটরিং ও পর্যালোচনার প্রক্রিয়া যাচাই ও এর যথার্থতা পরীক্ষাপূর্বক মূল্যায়ন করুন। | ৩ | | |
| | | ৪ | বিএফআইইউ কর্তৃক জারীকৃত নির্দেশনা এবং প্রতিষ্ঠানের নিজস্ব নীতিমালা অনুযায়ী মানিলন্ডারিং ও সন্ত্রাসে অর্থায়ন সংক্রান্ত ঝুঁকি প্রতিরোধে যথাযথ ব্যবস্থা গ্রহণ করা হয়েছে কিনা? BAMLCO কর্তৃক শাখায় পরিচালিত উচ্চ ঝুঁকিযুক্ত হিসাবসহ সকল হিসাবের লেনদেন মনিটরিং পর্যাপ্ত কি? | মানিলন্ডারিং ও সন্ত্রাসে অর্থায়ন সংক্রান্ত ঝুঁকি প্রতিরোধে শাখার গৃহীত পদক্ষেপ মূল্যায়ন করুন। BAMLCO কর্তৃক উচ্চ ঝুঁকিযুক্ত হিসাবসহ সকল হিসাবের লেনদেন মনিটরিং পদ্ধতি যাচাই ও এর যথার্থতা পরীক্ষাপূর্বক মূল্যায়ন করুন। | ৪ | | |
| | | ৫ | বিএফআইইউ মাস্টার সার্কুলার অনুসারে শাখায় PEPs প্রভাবশালী ব্যক্তি, আন্তর্জাতিক সংস্থার প্রধান বা উচ্চ পর্যায়ের কর্মকর্তার কোন হিসাব সংরক্ষণ করা হচ্ছে কিনা? | এ ধরনের হিসাব খোলা ও পরিচালনার ক্ষেত্রে বিএফআইইউ মাস্টার সার্কুলার অনুসারে সতর্কতা অবলম্বন করা হচ্ছে কিনা তা যাচাই করুন। তবে PEPs প্রভাবশালী ব্যক্তি, আন্তর্জাতিক সংস্থার প্রধান বা উচ্চ পর্যায়ের কর্মকর্তার কোন হিসাব না থাকলেও যদি বিএফআইইউ মাস্টার সার্কুলার এ প্রদত্ত নির্দেশনা বাস্তবায়নের প্রক্রিয়া বিদ্যমান থাকে তাহলে শাখা পূর্ণ নম্বর প্রাপ্ত হবে। | ৩ | | |



| | | | | | | | |
|---|---|---|---|---|---|--|--|
| | | ৬ | বিএফআইইউ প্রদত্ত সেলফ অ্যাসেসমেন্ট শাখা কর্তৃক কতটুকু সঠিক ও কার্যকরভাবে সম্পাদন হচ্ছে? | শাখার সেলফ অ্যাসেসমেন্ট রিপোর্ট পর্যালোচনা করুন। সঠিক ও কার্যকরভাবে সেলফ অ্যাসেসমেন্ট রিপোর্ট প্রণয়ন ও বাস্তবায়নের ভিত্তিতে নম্বর প্রদান করুন। | ৬ | | |
| ২ | মানি লন্ডারিং প্রতিরোধ ও সন্ত্রাসে অর্থায়ন প্রতিরোধ বিষয়ে কর্মকর্তাদের জ্ঞান ও সচেতনতা বৃদ্ধি এবং ঝুঁকি প্রতিরোধে গৃহীত ব্যবস্থা। | ১ | শাখায় কয়জন কর্মকর্তা/কর্মচারী মানি লন্ডারিং প্রতিরোধ ও সন্ত্রাসে অর্থায়ন প্রতিরোধ বিষয়ক আনুষ্ঠানিক প্রশিক্ষণ গ্রহণ করেছেন? | ১০০% কর্মকর্তার প্রশিক্ষণ সম্পূর্ণ হলে তা সন্তোষজনক বলে বিবেচিত হবে। প্রশিক্ষণের হার অনুসারে নম্বর প্রাপ্ত হবে। | ৩ | | |
| | | ২ | শাখার কর্মকর্তাগণ মানি লন্ডারিং ও সন্ত্রাসী কার্যে অর্থায়ন প্রতিরোধ বিষয়ে বিদ্যমান আইন, বিধিমালা, বিএফআইইউ কর্তৃক সময় সময় জারীকৃত নির্দেশনা ও গাইডেন্স নোটস এবং প্রতিষ্ঠানের নিজস্ব মানি লন্ডারিং প্রতিরোধ ও সন্ত্রাসে অর্থায়ন প্রতিরোধ নীতিমালা সম্পর্কে অবহিত আছেন কি? | শাখার সংশ্লিষ্ট কর্মকর্তাদের সাক্ষাৎকারের ভিত্তিতে মূল্যায়ন করুন। | ৪ | | |
| | | ৩ | মানি লন্ডারিং ও সন্ত্রাসে অর্থায়ন প্রতিরোধ কার্যক্রম মূল্যায়নের জন্য একটি ত্রৈমাসিক ভিত্তিতে শাখা ব্যবস্থাপকের নেতৃত্বে কর্মকর্তাগণের সভা আয়োজন করা হয় কিনা? | সভার আলোচ্যসূচী সংগ্রহ ও এর কার্যকারিতা পরীক্ষা করুন। | ৫ | | |
| | | ৪ | বিএফআইইউ কর্তৃক জারীকৃত নির্দেশনা এবং প্রতিষ্ঠানের নিজস্ব নীতিমালা অনুযায়ী মানি লন্ডারিং ও সন্ত্রাসে অর্থায়ন সংক্রান্ত ঝুঁকি প্রতিরোধে যথাযথ ব্যবস্থা গ্রহণ করা হয়েছে কিনা? | সাক্ষাৎকার ও নথিপত্রের ভিত্তিতে যাচাই করুন। | ৩ | | |
| ৩ | গ্রাহক পরিচিতি (KYC) পদ্ধতি | ১ | সকল প্রকার হিসাব খোলা ও লেনদেন পরিচালনার ক্ষেত্রে মানি লন্ডারিং প্রতিরোধ আইন, সন্ত্রাস বিরোধী আইন এবং বিএফআইইউ কর্তৃক জারীকৃত মাস্টার সার্কুলারের নির্দেশনা অনুসারে গ্রাহক পরিচিতি সন্তোষজনকভাবে গ্রহণ করা হয় কিনা ? | প্রত্যেক ধরনের ৪/৫ টি হিসাবের নমুনা পরীক্ষা করুন। নিম্নোক্ত বিষয়ে সন্তোষসাপেক্ষে নম্বর প্রদান করুন- গ্রাহক পরিচিতির যথার্থতা কিভাবে যাচাই করা হয়? কিভাবে তা শাখায় সংরক্ষণ করা হচ্ছে? KYC সম্পাদনকালে গ্রাহকের তহবিলের উৎস যাচাই করা হয়েছে কিনা? হিসাবের প্রকৃত সুবিধাভোগী (Beneficial Owner) সনাক্ত করা হয়েছে কিনা এবং তা যাচাই এর প্রক্রিয়া সন্তোষজনক কিনা? উচ্চ ঝুঁকিবিশিষ্ট গ্রাহকদের ক্ষেত্রে ঝুঁকির নিরিখে অতিরিক্ত তথ্য (EDD) সংগ্রহ করা হয় কি না? | ৬ | | |
| | | ২ | বিএফআইইউ কর্তৃক জারীকৃত মাস্টার সার্কুলারের নির্দেশনা অনুসারে শাখা যথাযথভাবে ঝুঁকির ভিত্তিতে তাদের গ্রাহকদের শ্রেণীবিন্যাস/ শ্রেণীকরণ করে কি? | বিএফআইইউ কর্তৃক জারীকৃত মাস্টার সার্কুলারের নির্দেশনা পরিপালিত হয় কিনা যাচাই করুন। | ৬ | | |
| | | ৩ | উচ্চ ঝুঁকিবিশিষ্ট গ্রাহকদের ক্ষেত্রে প্রয়োজনীয় অতিরিক্ত তথ্য সংগ্রহ করা হয় কি? | কি ধরনের তথ্য সংগ্রহ করা হয় এবং তা যথেষ্ট কিনা পরীক্ষা করুন। | ৫ | | |
| | | ৪ | শাখা কি গ্রাহকের KYC Profile নির্দিষ্ট সময় পর পর পুনঃমূল্যায়নপূর্বক হালনাগাদ করে থাকে? | KYC Profile পুনঃমূল্যায়ন ও হালনাগাদ পদ্ধতি মূল্যায়ন করুন। | ৫ | | |



| | | | | | | | |
|---|---|---|--|---|---|--|--|
| ৪ | সন্ত্রাস বিরোধী আইন, ২০০৯ এর পরিপালন | ১ | সন্ত্রাস বিরোধী আইন, ২০০৯ এর অধীন সন্ত্রাসে অর্থায়ন প্রতিরোধের লক্ষ্যে শাখা কী ধরনের কার্যকর পদক্ষেপ গ্রহণ করেছে? | নিম্নোক্ত বিষয়ে সন্ত্রাসসাপেক্ষে নম্বর প্রদান করুন- জাতিসংঘের নিরাপত্তা পরিষদের বিভিন্ন রেজুলেশনের আওতায় সন্ত্রাস, সন্ত্রাসী কার্য ও ব্যাপক ধ্বংসাত্মক অস্ত্র বিস্তারে অর্থায়নে জড়িত সন্দেহে তালিকাভুক্ত কোন ব্যক্তি বা সত্তা এবং বাংলাদেশ সরকার কর্তৃক তালিকাভুক্ত কোন ব্যক্তি বা নিষিদ্ধ ঘোষিত সত্তার নামের তালিকা শাখায় সংরক্ষণ ও তদানুসারে হিসাব ও লেনদেন কার্যক্রম যাচাই করা হয় কিনা? শাখা এ বিষয়ক নিজস্ব কোন Mechanism অনুসরণ করে কিনা? এরূপ ব্যক্তি বা সত্তার নামে শাখায় পরিচালিত হিসাবের (যদি থাকে) বিষয়ে বিএফআইইউ কে অবহিত করা হয় কিনা? | ৫ | | |
| ৫ | সন্দেহজনক লেনদেন রিপোর্ট (STR) ও নগদ লেনদেন রিপোর্ট (CTR) | ১ | শাখার কর্মকর্তাগণ সন্দেহজনক লেনদেন রিপোর্ট (STR) সম্পর্কে অবহিত আছেন কি? | শাখায় সন্দেহজনক লেনদেন Reporting এর জন্য Internal Reporting Mechanism চালু আছে কিনা? তা সকল কর্মকর্তা জানেন কিনা? | ৫ | | |
| | | ২ | শাখায় মানি লন্ডারিং ও সন্ত্রাসে অর্থায়ন সংক্রান্ত সন্দেহজনক লেনদেন চিহ্নিতকরণের কার্যকর পদ্ধতি চালু আছে কি? এ যাবৎ কতগুলো সন্দেহজনক লেনদেন (STR) BAMLCO কর্তৃক CCU এর নিকট রিপোর্ট করা হয়েছে? | শাখায় সন্দেহজনক লেনদেন সংঘটিত হওয়া সত্ত্বেও যদি BAMLCO কর্তৃক CCU এর নিকট কোন STR না করা হয়ে থাকে তাহলে তা অসন্তোষজনক বিবেচিত হবে। নথি ও সিস্টেম পরীক্ষা করে শাখায় STR সনাক্তকরণের জন্য কোন পদ্ধতির প্রবর্তন করা হয়েছে কিনা তা যাচাই করুন। নিম্নোক্ত বিষয়ে সন্ত্রাস সাপেক্ষে নম্বর প্রদান করুন- শাখায় সন্দেহজনক লেনদেন চিহ্নিত করার কোন পদ্ধতি অনুসরণ করা হয় কিনা? শাখা পর্যায়ে নিম্নলিখিত Internal Report যথাযথভাবে সংরক্ষণ করা হয় কিনা? | ৪ | | |
| | | ৩ | শাখা কর্তৃক যথাযথ ও সঠিকরূপে নগদ লেনদেন রিপোর্ট (CTR) করা হয় কিনা? | এতদসংক্রান্ত নথি পরীক্ষা করুন। (কমপক্ষে এক মাসের নগদ লেনদেন) ক্যাশ রেজিস্টার/বিবরণী হতে পরীক্ষা করুন এবং এর ভিত্তিতে ঐ মাসে দাখিলকৃত CTR রিপোর্ট এর পরীক্ষাপূর্বক মূল্যায়ন ও এর সঠিকতার বিষয়ে মূল্যায়ন করুন। | ২ | | |
| ৬ | CCU বরাবর বিবরণী দাখিল | ১ | শাখা কর্তৃক কতটি বিবরণী CCU বরাবর দাখিল করা হয়? শাখা কি যথাসময়ে বিবরণী দাখিল করে? | এতদসংক্রান্ত নথি পরীক্ষা করুন। বিলম্বে অথবা বিবরণী দাখিল না করলে তা অসন্তোষজনক বিবেচিত হবে। | ৩ | | |
| | | ২ | শাখা কর্তৃক নিয়মিতভাবে সেলফ্ অ্যাসেসমেন্ট করা হয় কিনা? প্রস্তুতকৃত বিবরণী যথাযথ কিনা? | এতদসংক্রান্ত বিবরণী পরীক্ষা করুন। তথ্যাদি সঠিক ও পরিপূর্ণ না হলে তা অসন্তোষজনক বিবেচিত হবে। | ৩ | | |
| ৭ | রেকর্ড সংরক্ষণ | ১ | গ্রাহক পরিচিতি (KYC) এবং লেনদেন সম্পর্কিত রেকর্ড যথাযথভাবে সংরক্ষণের বিধান আছে কি? | ৫টি বন্ধ হিসাব পরীক্ষা করুন। এক্ষেত্রে মানি লন্ডারিং প্রতিরোধ আইন এর বিধান যথাযথভাবে অনুসরণ করা হয়েছে কিনা যাচাই করুন। | ৪ | | |



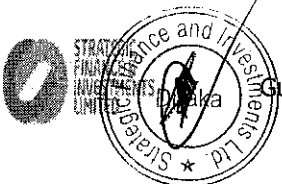
| | | | | | | | |
|---|---------------------------------------|---|---|---|-----|--|--|
| | | ২ | নিয়ন্ত্রণকারী কর্তৃপক্ষ বা CCU এর চাহিদা মোতাবেক রেকর্ডসমূহ সরবরাহ করা হয় কি? | এতদসংক্রান্ত নথি পরীক্ষা করুন। যথাসময়ে ও যথাযথ তথ্য সরবরাহ না করলে তা অসন্তোষজনক বিবেচিত হবে। | ৩ | | |
| ৮ | AML সম্পর্কিত শাখার সার্বিক কার্যক্রম | ১ | শাখা ব্যবস্থাপক BAMLCO না হলে শাখা ব্যবস্থাপক AML প্রোগ্রাম বাস্তবায়নে যথাযথ ভূমিকা পালন করে কি? | শাখায় আয়োজিত সভার আলোচ্যসূচী ও শাখা ব্যবস্থাপকের সাথে সাক্ষাৎকারের ভিত্তিতে মূল্যায়ন করুন। | ৫ | | |
| | | ২ | পূর্ববর্তী অভ্যন্তরীণ ও বহিঃ নিরীক্ষা প্রতিবেদন পরীক্ষাকালে অগত্যা প্রোগ্রামের আওতায় কোন অনিয়ম ও দুর্বলতার উল্লেখ পাওয়া গেছে কিনা এবং শাখা কোন সংশোধনমূলক ব্যবস্থা গ্রহণ করেছে কিনা? | সর্বশেষ নিরীক্ষা সংক্রান্ত রিপোর্ট পরীক্ষা করুন এবং কি ধরনের সংশোধনমূলক ব্যবস্থা নেওয়া হয়েছে যাচাই করুন। | ৪ | | |
| | | ৩ | শাখার সার্বিক কার্যক্রম সন্তোষজনক কি? | শাখার মানি লডারিং ও সন্ত্রাসে অর্থায়ন প্রতিরোধ সংক্রান্ত সার্বিক কার্যক্রম এবং শাখা ব্যবস্থাপকের পারফরম্যান্সের ভিত্তিতে মূল্যায়ন করুন। | ৬ | | |
| | | | | মোট | ১০০ | | |

শাখার সার্বিক মূল্যায়নঃ

| স্কোর | রেটিং |
|--------------|--------------|
| ৯১-১০০ | শক্তিশালী |
| ৭১-৯০ | সন্তোষজনক |
| ৫৬-৭০ | মোটামুটি ভাল |
| ৪১-৫৫ | প্রান্তিক |
| ৪০ ও এর নিচে | অসন্তোষজনক |

শাখার অবস্থানঃ

| প্রাপ্ত স্কোর | রেটিং |
|---------------|-------|
| | |



Internal Suspicious Activity Report Form

A. Reporting Institution :

1. Name of the FI:

2. Name of the Branch:

B. Details of Report:

1. Date of sending report:

2. Is this the addition of an earlier report? Yes No

3. If yes, mention the date of previous report

C. Suspect Account Details :

1. Account Number:

2. Name of the account:

3. Nature of the account:
(FDR/loan/other, pls. specify)

4. Nature of ownership:
(Individual/proprietorship/partnership/company/other, pls. specify)

5. Date of opening:

6. Address:

D. Account holder details :

1. Name of the account holder:

2. Address:

3. Profession:

4. Nationality:

5. Other accounts number (if any):



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

E. Introducer Details :

- 1. Name of introducer:
- 2. Account number:
- 3. Relation with account holder:



4. Address:

5. Date of opening:

6. Whether introducer is maintaining good relation with FI:

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

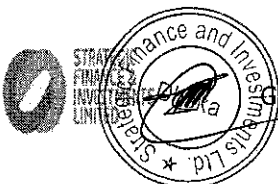
- a. Identity of clients
- b. Activity in account
- c. Background of client
- d. Multiple accounts
- e. Nature of transaction
- f. Value of transaction
- g. Other reason (Pls. Specify)

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

G. Suspicious Activity Information

Summary characterization of suspicious activity:

- | | | |
|--|---|--|
| a. <input type="checkbox"/> Bribery/Gratuity | h. <input type="checkbox"/> Counterfeit debit/credit card | o. <input type="checkbox"/> Mortgage Loan Fraud |
| b. <input type="checkbox"/> Check Fraud | i. <input type="checkbox"/> Counterfeit instrument | p. <input type="checkbox"/> Mysterious Disappearance |
| c. <input type="checkbox"/> Check Kitting | j. <input type="checkbox"/> Credit card fraud | q. <input type="checkbox"/> Misuse of Position or Self-Dealing |



- d. Commercial loan fraud k. Debit card fraud r. Structuring
- e. Computer intrusion l. Defalcation/Embezzlement s. Terrorist Financing
- f. Consumer loan fraud m. False statement t. Wire Transfer Fraud
- g. Counterfeit check n. Identity Theft u. Other _____

| H. Transaction Details: | | | |
|-------------------------|------|--------|-------|
| Sl. no. | Date | Amount | Type* |
| | | | |
| | | | |
| | | | |
| | | | |

*Cash/Transfer/Clearing/DD/PO/etc.

Add paper if necessary

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

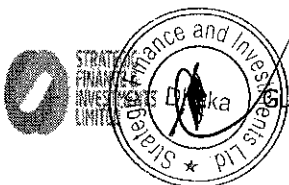
J. Has the suspicious transaction/activity had a material impact on or otherwise affected the financial soundness of the FI?

Yes No

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

L. Documents to be enclosed

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



To whom it may concern

Statement of Compliance

I do hereby declare & confirm that as an employee of SFIL:

- a) Have read the Company's Guidelines on "Prevention of Money Laundering and Combating Terrorist Financing"; as well as circulars/directives of Bangladesh Financial Intelligence Unit (BFIU) and Government's Acts on Anti-Money Laundering and Anti-Terrorism and understood the implications thereof;
- b) Shall comply the applicable laws and regulations and corporate ethical standards;
- c) Shall comply all the rules and regulations in the normal course of my assignments. It is my responsibility to become familiar with the rules and regulations that relate to my assignment; and
- d) Shall be held responsible for carrying out compliance responsibilities on prevention of Money Laundering and combating Terrorist Financing meticulously.

Signature:

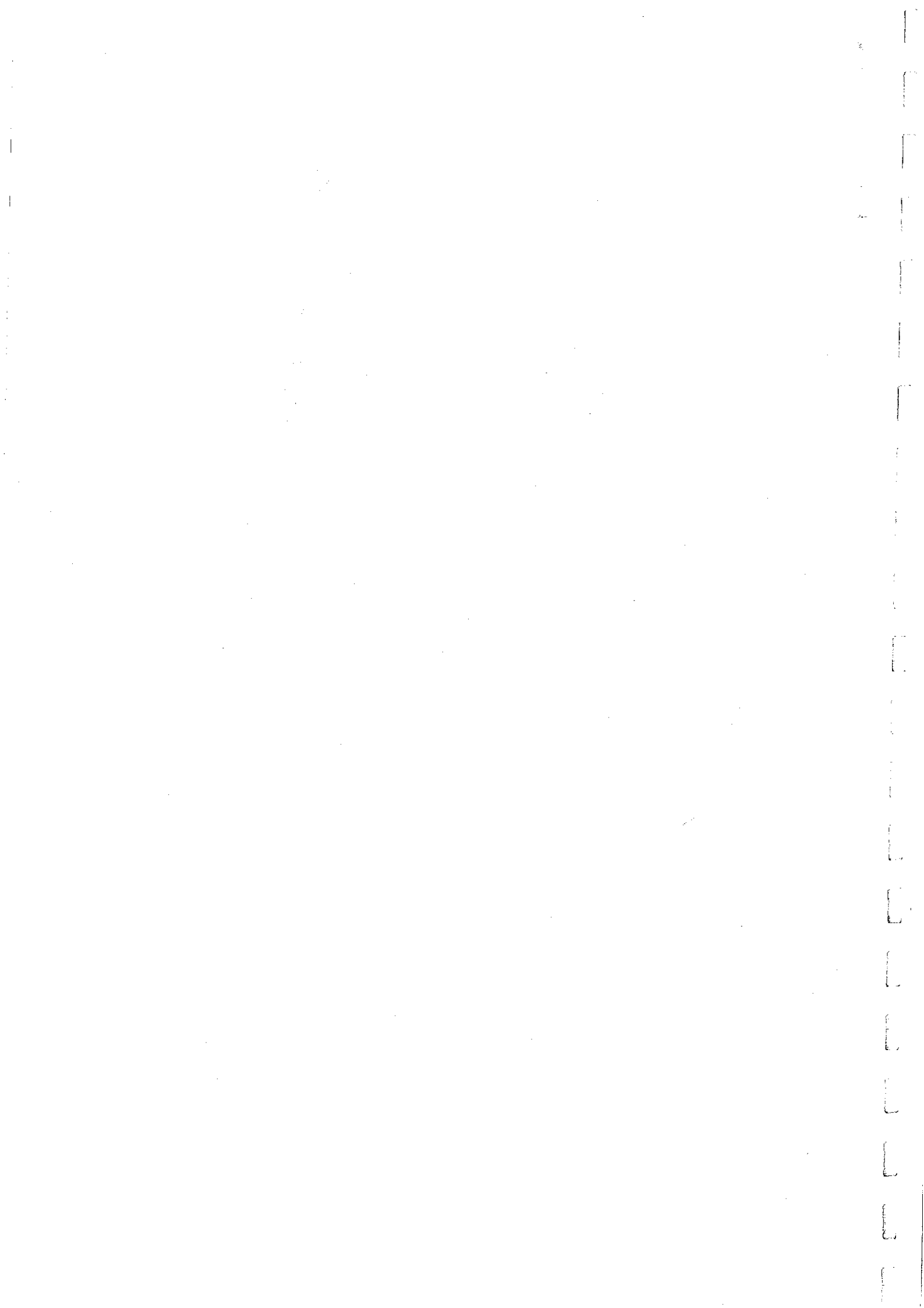
Name:

Designation:

Department:

Job location:





Relevant extract copy of the minutes of 9th Board Meeting of Strategic Finance & Investments Limited held on January 22, 2021 at 9:00 AM in Head Office through physical & virtual meeting.


BMA-09-10 : Approval of Guidelines on Prevention of Money Laundering and Terrorist Financing;

DISCUSSION:

The Board reviewed the Guidelines on Prevention of Money Laundering and Terrorist Financing.

RESOLVED THAT:

The Guidelines on Prevention of Money Laundering and Terrorist Financing is hereby approved.


Mohammad Razibuzzaman Khan
Company Secretary



