Guidance on Reporting
Suspicious Transaction Report
for
The Reporting Organization

Bangladesh Financial Intelligence Unit

January 2019

Table of Contents

A. Preamble

This document is issued as per power conferred in Section 23(1)(d) of Money Laundering Prevention Act, 2012 (MLPA) and in Section 15(1)(d) of Anti Terrorism Act, 2009 (ATA) for all the reporting organizations defined under Section 2(w) of MLPA and Section 2(20) of ATA.

The purpose of this guidance note is to assist the Reporting Organizations (RO) to obtain a practical and comprehensive approach in recognizing and reporting suspicious activity as the ROs are obligated to submit Suspicious Transaction Report (STR)/ Suspicious Activity Report (SAR) to Bangladesh Financial Intelligence Report (BFIU) required under the MLPA, 2012 and ATA, 2009 and the BFIU Directives for the prevention of Money Laundering and Terrorist Financing.

The Money Laundering and Terrorist Financing (ML/TF) is an ever evolving process and individuals involved in such activities are continually attempting to exploit services and products offered by Financial Institutions and Designated Non Financial Businesses and Professions (DNFBP) in an effort to disguise the true nature of their illicit proceeds. This guidance note is a summary of non-exhaustive steps and best practices to be adopted by the ROs when dealing with the execution and/or review of clients' transactions and activities and the assessment of suspicion.

B. Reporting Requirement

Suspicious activity can be identified both during the on-boarding or ongoing due diligence of a client as well as during the transaction monitoring process and may be raised by any employee of a reporting organization.

Under Section 25(1)(d) of MLPA, 2012, ROs shall have to report any doubtful transaction or attempt of such transaction as defined under Section 2(z) of the same act as suspicious transaction report to the BFIU immediately on its own accord.

Definition of Suspicious Transaction

As per Section 2(z) of MLPA 2012 Suspicious Transaction means such transactions

- which deviates from usual transactions
- of which there is ground to suspect that
    - The property is the process of an offense
    - It is financing to any terrorist activity, a terrorist group or an individual terrorist
- Which is for the purpose of this Act, any other transaction or attempt of transaction delineated in the instruction issued by BFIU from time to time.

As per Section 2(16) of ATA, 2009, Suspicious Transaction means such transactions

- which deviates from usual transactions
- Which invokes presumption that
    - it is the proceeds of an offence under this Act
    - it relates to financing of terrorist activities or a terrorist person or entity

- For the purpose of this Act, any other transaction or attempt of transaction delineated in the instruction issued by BFIU from time to time.

Suspicious Activity (SA) arises from suspicion relating to general behavior of the person in question which creates the knowledge or belief that he or she may be involved in illegal activities out of which proceeds might be generated. Any suspicious attempted transaction also fall in this category.

C. Reporting Process

The final output of an Anti Money Laundering (AML) & Combating Financing of Terrorism (CFT) compliance program 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 AML & CFT risk for ROs. Therefore it is necessary to find out the suspicious transaction and suspicious activity for the safety and soundness of the ROs.

In order to prepare an effective intelligence report or to have leads for a quality report, a complete STR is an essential requirement, i.e. the information submitted must be sufficient and complete to establish a connection to be made between the person(s) and the suspicious activity/transaction.

Generally STR/SAR means a formatted report of suspicious transactions/activities where there is reasonable grounds to believe that funds are the proceeds of predicate offence or may be linked to terrorist activity or the transactions are not seems to be usual manner. Such report is to be submitted by ROs to the competent authorities i.e. to BFIU. Suspicion basically involves a personal and subjective assessment. The reporting organizations have to assess whether there are reasonable grounds to suspect that a transaction is related to money laundering offence or a financing of terrorism offence.

In case of reporting of STR/SAR, reporting organizations should conduct the following 3 stages:

C.1. Identification of STR/SAR

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

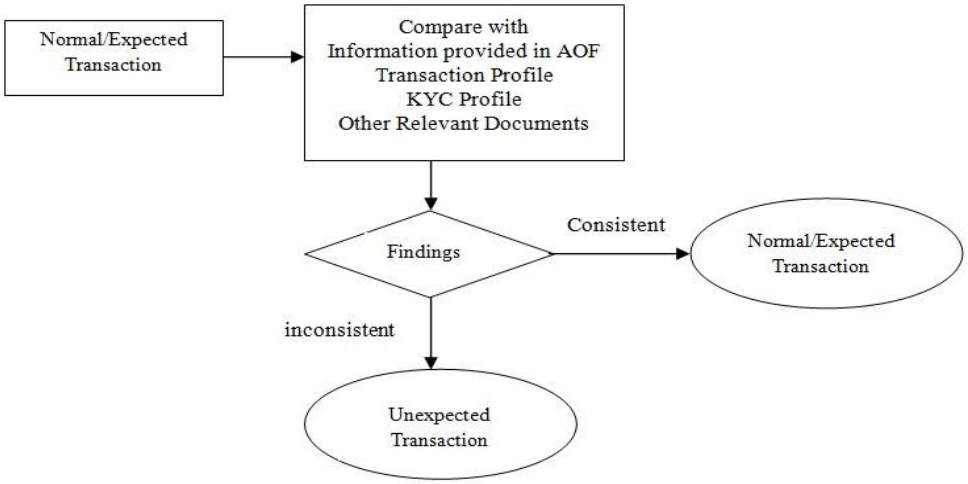
- Comparing the KYC profile, if any inconsistency is found and there is no reasonable explanation;
- By monitoring customer transactions;
- By using red flag indicators.

A transaction which appears unusual is not necessarily suspicious. Even customers with a stable and predictable transaction profiles will have periodic transactions that are unusual for them. Many customers will, for perfectly good reasons, have an erratic pattern of transactions or account activity. So the unusual is, in the first instance, only a basis for further enquiry,

which may in turn require judgment as to whether it is suspicious. A transaction or activity may not be suspicious at the time, but if suspicions are raised later, an obligation to report then arises. **Section-I** provides some red flag indicators for identifying STR/SAR related to ML & TF.

All suspicions reported to the CCU should be documented, or recorded electronically. The report should include full details of the customer who is the subject of concern and as full a statement as possible of the information giving rise to the suspicion. All internal enquiries made in relation to the report should also be documented. This information may be required to supplement the initial report or as evidence of good practice and best endeavors if, at some future date, there is an investigation and the suspicions are confirmed or disproved.

The following chart shows the graphical presentation of identification of STR/SAR-



This stage is very vital for STR/SAR reporting. Depending on size, need and complexity of ROs monitoring of unusual transactions may be automated, manually or both. Some ROs use specialized software to detect unusual transactions or activities, however, the use of such software can only be complemented managerial oversight and not be replaced the need for constant monitoring of the accounts of customers. Monitoring mechanisms should be more rigorous in high-risk areas of a RO and supported by adequate information systems to alert management and other appropriate staffs of unusual /suspicious activity. Training of staff in the identification of unusual /suspicious activity should always be an ongoing activity.

C.2. Evaluation

This part must be in place at branch level. After identification of STR/SAR at branch level, BAMLCO shall evaluate the reported transaction or activity in an appropriate manner and shall preserve his observations on it in a written format. If the transaction or activity seems to be suspicious, it, along with all necessary supportive documents, has to be sent to the Central Compliance Committee/Central Compliance Unit/Money Laundering and Terrorist Financing Prevention Department/Division without any delay. After receiving report from branch, Money Laundering and Terrorist Financing Prevention Department/Division shall review whether the reported suspicious transaction

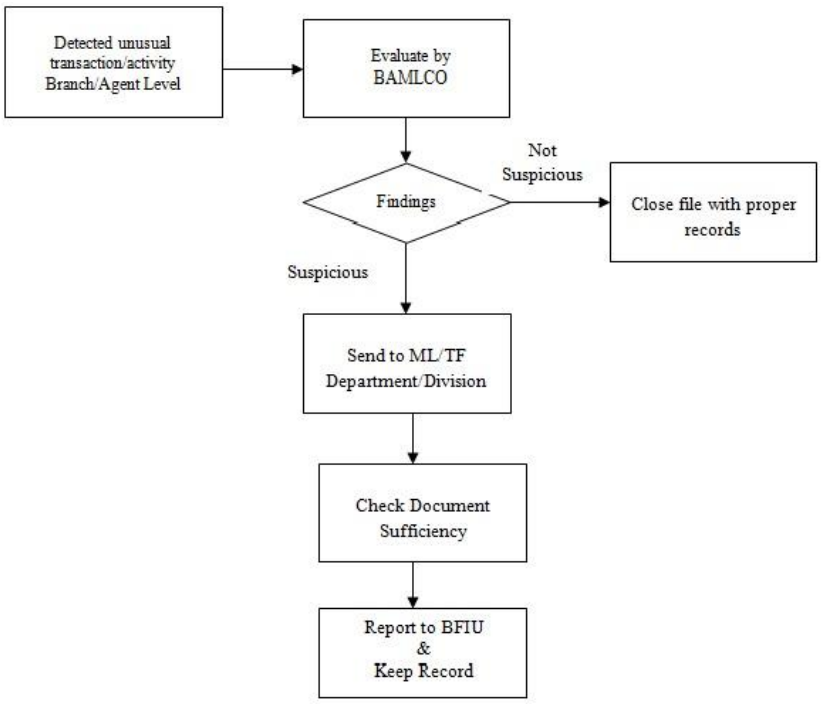
or activity from the branch has been reported in an appropriate manner with all necessary information, data and documents.

C.3 Disclosure

This is the final stage and ROs should submit STR/SAR to BFIU. After checking the sufficiency of the required documents, Central Compliance Committee/Central Compliance Unit/Money Laundering and Terrorist Financing Prevention Department/Division shall submit a suspicious transaction/activity report to BFIU without delay by using goAML web as per instruction mentioned in goAML Manual. Every stages of evaluation ROs should keep records with proper manner.

Central Compliance Committee/Central Compliance Unit/Money Laundering and Terrorist Financing Prevention Department/Division shall submit suspicious transaction/activity report to BFIU if it identifies any transaction or activity as suspicious even though the concerned branch did not identified as suspicious

For simplification, the flow chart given below shows overall STR/SAR evaluation and reporting procedures:



D. Documenting Reporting Decisions

In order to control legal risks or for future reference it is important that adequate records of SARs and STRs are kept. This is usually done by the CAMLCO and would normally include details of:

a) All SARs / STRs made;
b) How the BAMLCO handled matters, including any requests for further information
c) Assessments of the information provided, along with any subsequent decisions about whether or not to await developments or seek additional information;
d) The rationale for deciding whether or not to proceed with SAR/STR;
e) Any advice given or action taken about continuing the business relationship and any relevant internal approvals granted in this respect.

These records can be simple or sophisticated, depending on the size of the business and the volume of reporting, but they always need to contain broadly the same information and be supported by the relevant working papers. The maintenance and retention of such records is important as they justify and defend the actions taken by the BAMLCO and/or other members of staff and should be made available to the Competent Authorities and BFIU upon request.

For practical purposes and ease of reference, a reporting index could be kept and each SAR/STR could be given a unique reference number.

E. Reporting Guidance

BFIU implemented a secured online reporting system namely the goAML, which requires the ROs to submit SARs and STRs through this channel. The goAML Web application provides a secure web based interface between the BFIU and its reporting organizations for the electronic upload of reports such as XML files, filling out the online report forms or sending XML files as attachments by secure e-mail, information sharing among stakeholders and other information.

ROs shall submit STR/SAR by using goAML web as per instruction mentioned in goAML Manual. (https://www.bb.org.bd/eservices.php). ROs can also submit STR/SAR manually by using the format prescribed by BFIU (https://www.bb.org.bd/bfiu/reporting_forms.php). ROs shall preserve all information on a reported STR until any further instruction by BFIU.

E.1. Some Special Scenarios for Reporting

(1) If a reporting organization fails to perform conducting Customer Due Diligence (CDD) due to the non cooperation of customer and the collected information/data of the customer appears unreliable, reporting organization should submit suspicious transaction/activity report on such customers;

(2) If Reporting Organization identifies any account or transaction in the name of listed or proscribed person or entity under any United Nations Security Council Resolution or any person or entity listed or proscribed by Bangladesh Government or any individual or entity directly or indirectly under their control or association, Reporting Organization must stop transaction of the account and report BFIU with detailed information within the next working day;

(3) If any news on Financing of Terrorism and Financing of Proliferation of Weapons of Mass Destruction is published in the media and if any account of any person or entity related to that activity is maintained with the reporting organization, detailed information must be reported to BFIU without any delay.

F. Tipping Off

A 'tipping off' offence occurs when any person discloses, either to the person who is the subject of a suspicion or any third party, that:

a) Information or documentation on ML/TF has been transmitted to BFIU;

b) A SAR/STR has been submitted internally or to BFIU;

c) Authorities are carrying out an investigation/search into allegations of ML/TF;

Tipping-off may also occur in those cases when an employee approaches the client to collect information about the internal on-going investigation, and through the intense questioning, the client becomes aware of the investigation.

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

Reporting Organizations shall consider the confidentiality of the reporting of STR/SAR. They should not make any behavior or performance that could tip-off the customer and he/she (the customer) could be cautious.

Reporting Organizations shall report suspicious transaction/activity without performing Customer Due Diligence (CDD) if there is reasonable ground that Tipping Off may take place in the event of performing CDD for any transaction suspected to be related to ML & TF.

G. Penalty

As per Section 25 (2) of MLPA, if any reporting organization fails to report STR/SAR, a fine of at least taka 50 (Fifty) Thousand but not exceeding taka 25 (Twenty Five) lacs can be imposed on the reporting organization. In addition to the fine, BFIU may 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 cause may be, shall inform the registration or licensing authority about the fact so as to be relevant authority may take appropriate measures against the organization.

G.1. Penalty of Tipping Off

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

H. Safe Harbor Provision

In section (28) of MLPA, 2012 provides the safe harbor for persons submitting suspicious reports.

As per Section 28 of MLPA, no suit or prosecution or administrative measures or any other legal proceedings shall lie against any reporting organization or its Board of Directors or any of its officers or staffs 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.

Disclosure of information in good faith by a reporting organization or by an employee or director of such a reporting organization shall not constitute a breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, and shall not involve the obliged entity or its directors or employees in liability of any kind even in circumstances where they were not precisely aware of the underlying criminal activity and regardless of whether the illegal activity actually occurred.

I. Red Flags

Suspicion can be defined as

- A state of mind more definite than speculation but falling short of evidence-based knowledge;
- A positive feeling of actual apprehension or mistrust;
- A slight opinion, without sufficient evidence.

The following red flags can be used as indicators of Suspicious Transaction or Suspicious Activities:

1. Significant mismatch with financial status of the customer.

2. Fake documents & false information submitted by the customer.

3. Customer is reluctant to provide documents.

4. Frequent cash transaction not aligned with the business or, profession of the customer.

5. Structuring.

6. Pay order & Demand Draft purchased or/and encashed without bona fide transaction.

7. Cheque kitting and fraudulent activity related to financial instruments.

8. Large number and amount of transaction with minimum balance.

9. Sudden pay off of loan or, multiple number of unpaid installments.

10. Account opened and transacted large amount in the name of non-earning members and close aides.

11. Customer or beneficiary has link with terrorist activities or, terrorist financing or, sanctioned organization.

12. Adverse media report against the customer or, beneficiary.

13. Transaction or activities related to TBML/TF related trade financing.

14. Transaction with high risk jurisdiction.

15. Suspicious cross border inward/ outward transaction.

16. Relationship with front company or Shell Company.

17. Use of funds by the NGO/NPO/ Co-operative inconsistent with the purpose.

18. An atypical incidence of pre-payment of insurance premiums.