Anti–Money Laundering Central Board

Financial Intelligence Unit

Instruction No. 2/2019

Nay Pyi Taw, the 15th Waning of Tazaungmon 1381 ME

Suspicious Transaction Report Guideline

(26th November 2019)

Introduction

1. According to section 3 (e) of the Anti–Money Laundering Law, Pyidaungsu Hluttaw Law No.11 (2014), the reporting organizations including banks and financial institutions should report the transactions relating to the suspicious findings in line with the section 32, 34 of the Anti–Money Laundering Law and rules 48, 49, 50 of the Anti–Money Laundering Rules to Financial Intelligence Unit–FIU.

2. In addition, according to section 69 (c) of the Anti–Money Laundering Law, Financial Intelligence Unit has to issue the required directive, regulations and principles by the approval of the Anti–Money Laundering Central Board in order to implement the provisions of the Anti–Money Laundering Law.

3. Therefore Financial Intelligence Unit prepared this guidance note to assist banks and financial institutions as well as government agencies and supervisors while identifying and reporting suspicious financial transactions and suspicious financial activities in order to prevent and mitigate the money laundering and funds for terrorism financing.

Purpose

4. To understand and identify the nature of suspicious financial transactions and activities and to submit the quality suspicious transaction reports to Financial Intelligence Unit while reporting by reporting organizations in line with the reporting obligations of the Anti–Money Laundering Law.

Reporting Requirements for Suspicious Activities

5. 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 found at social media.

6. Regarding to report the suspicious transaction, the provisions are described in section 32, 34 of the Anti–Money Laundering Law and rules 48, 49, 50 of the Anti–Money Laundering Rules. There may be two conditions, attempted transaction (Suspicious Activity) and completed transaction (Suspicious Transaction), to be suspicious a transaction. 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 revenue might be generated. Suspicious Transaction (ST) arises from the suspicion created by a specific ***transaction***, which creates the knowledge or belief that the transaction may relate to the legitimization of proceeds from illegal activities.

7. According to section 32 of the Anti–Money Laundering Law, reporting organization should report promptly to Financial Intelligence Unit, if there is a reasonable suspicious ground to believe that money or property involved in transaction is obtained by illegal means or related to money laundering or terrorist financing, or attempted to do so. In section 46 of the Anti–Money Laundering Law, it is described that any responsible person from the reporting organization, in reporting to Financial Intelligence Unit under section 32, presents false statement or conceals facts shall, on conviction, be punished with imprisonment from a minimum of three years to a maximum of seven years and may also be liable to a fine. If the offender is a company or an organization, a fine which may extend to three hundred million kyats shall be imposed on such company or organization.

8. In order for a report to be useful for analysis and processing, it needs to be a quality report, i.e. the information submitted must be sufficient and complete to enable a connection to be made between the person(s) and the suspicious activity/transaction.

Anti–Money Laundering Compliance Officer's (AMLCO) Responsibilities

9. According to section 28 (b) of the Anti–Money Laundering Law, reporting organizations shall designate a compliance officer at the senior management level and ensure power to access any documents, records, registers and accounts necessary for the performance of his tasks; power to request and access any

information, notice, explanation or document from any employee of the reporting organization to compliance officer.

10. The compliance officer is considered to be the contact point for all AML issues for internal purposes and external authorities and should have the responsibility for reporting suspicious activity/transactions to FIU. Each obliged entity has the responsibility to notify FIU about the appointment. The compliance officer must develop an effective suspicious activity monitoring and reporting policy and create a culture of compliance, ensuring that staffs adhere to the firm's policies, procedures and processes designed to limit and control risks. Such policies, controls and procedures should be proportionate to the nature and size of the obliged entities. The compliance officer should also establish an internal reporting procedure that enables relevant employees to disclose their knowledge or suspicions of ML/TF as soon as it is practically possible by filing an Internal Suspicion Report. The compliance officer has the duty to validate and consider the information received through the Internal Suspicion Report by reference to any other relevant information, including monitoring and investigating transactions and discuss the circumstances of the case with the reporting employee concerned and, where appropriate, with the employee's superior(s). The evaluation of the information reported to the Compliance Officer should be recorded and retained on file. The compliance officer should assess the activity or transaction as suspicious; he/she has the obligation to file a SAR or a STR accordingly to FIU the soonest possible. The way to report is described in order no. 1/2019, the Reporting Obligation Guideline, of Financial Intelligence Unit.

Staff Training

11. The compliance officer is the person responsible to determine whether the firm's employees have the necessary knowledge on combating Money Laundering and Terrorist Financing or whether further training is required. A successful training program should be ongoing and not only meet the standards set out in the laws and regulations that apply to the obliged entities but should also satisfy internal policies and procedures and should mitigate the risk of getting caught up in a money laundering scandal. Training is one of the most important ways to convey the

importance of AML efforts, as well as educating employees about what to do if they encounter potential money laundering. The term 'training' includes, other than formal training courses, communication that serves to educate and inform employees, such as emails, newsletters, guidance notes, periodic team meetings and anything else that facilitates the sharing of information. Firms should firstly identify the target audience and each department/position should be trained on topics and issues that are relevant to them. After the target audience is identified, the next step is selecting the training topics (e.g. general information, legal framework, penalties from AML violations, how to react, internal policies, procedure for reporting suspicious activity internally within the firm, practical case studies of suspicious activity etc.). In addition, to achieve an effective training program, trainers need to consider and plan the timing, location and means of training.

Reporting Process

12. Suspicious or unusual transaction reporting process includes:

(a) Procedures to identify suspicious or unusual transactions or activity through various channels including employee observations or identification, inquiries from law enforcement or alerts generated by transaction monitoring systems;

(b) A formal evaluation of each instance, and continuation, of unusual transactions or activity;

(c) Documentation of the suspicious transaction reporting decision (i.e. irrespective of whether a report was submitted to the authorities);

(d) Procedures to periodically notify senior management or the board of directors of suspicious transaction submissions; and

(e) Employee training on detecting suspicious transactions or activity.

Documenting Reporting Decisions

13. In order to control legal risks, it is important that adequate records of internal SARs and STRs are kept. This is usually done by the compliance officer and would normally include details of:

(a) All internal SARs / STRs made;

(b) How the AMLCO 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 an external SAR/STR;

(e) Any advice given to engagement teams about continuing the business relationship and any relevant internal approvals granted in this respect.

14. 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 AMLCO and/or other members of staff and should be made available to the Competent Authorities and FIU upon request. For practicality purposes and ease of reference, a reporting index could be kept and each internal SAR/STR could be given a unique reference number.

Red Flags / Examples of Suspicious Activity (SA) and Suspicious Transaction (ST)

15 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. Suspicion is not a mere idle wondering, a vague feeling of unease.

16 **Suspicious Customer Behavior**

(a) Overly secretive client

(b) Client refuses to provide information

(c) Client shows familiarity with process

(d) Client has used/changed a number of advisors in short space of time

(e) Client appears disinterested with outcome

(f) Client is prepared to pay substantial abnormally high fees

(g) Client shows inadequate knowledge of transactions

(h) Client uses multiple bank accounts

(l) Client requests an unusual short or deferred repayment schedule

(j) Client does not want to receive correspondence to home address

(k) Client avoids face–to–face meetings

17. **Suspicious Customer Identification Circumstances**

(a) Client provides counterfeit documents

(b) Client only provides copies rather than original documents

(c) Client only provides foreign, unverifiable identity documents

(d) Client only acts through a third party

18. **Suspicious Employee Activity;** Eagerness to work long hours when the office is closed or take on additional work from other colleagues.

19. **Suspicious economic profile;**

(a) There is lack of sensible/commercial/financial or legal reason for business

(b) Absence of documentation to support a client's claims

(c) Business cannot be found on the internet

(d) Creation of complicated ownership structures

(e) Funds invested in dormant companies

(f) Transactions involve non–profit or charitable organizations for which there appears to be no logical economic purpose

20. **Suspicious Transactions**

(a) Large cash transactions/exchange of small bills for large ones

(b) Multiple transactions in a short period of time

(c) Finance is not provided by a credit institution

(d) Transfer of large amounts of money to or from overseas locations with instructions for payments in cash

(e) Cash deposits/withdrawals that fall consistently below the relevant transaction threshold

(f) Mortgages are repeatedly repaid quickly

(g) Unusual source of funds

(h) Request for payments to third parties

(l) Client receives high injection of capital

(k) Back to back property transactions

21. **Suspicion on terrorist financing and weapon proliferation**

(a) Client conducts uncharacteristic purchases (camping gear, weapons, hydrogen peroxide)

(b) Client trades in commodities that may be dual used in chemical and biological weapons

(c) Client donates to a cause that is subject to derogatory publicly available information (NPO's, NGO's, charity

22. **Suspicious Customer Relations**

(a) Parties connected without an apparent business reason

(b) Client is known to have convictions or currently under investigation

(c) Age of parties is unusual for type of transactions

(d) Client has known connections with criminals

Determine whether to report or not

23. In making a decision on whether to make a report, the following factors will need to be taken into account:

(a) Whether or not the activities/transactions in question consist of instances of reportable (suspected) ML/TF.

(b) Whether the information was obtained in circumstances where they are subject to professional secrecy or legal professional privilege

(c) Whether unusual activity appears during the ongoing monitoring of a client's information (i.e. the activity of the client is not in line with the initially documented economic profile).

(d) A STR may also be required when there are "reasonable grounds" to know or suspect. This is an objective test, i.e. the standard of behavior expected of a reasonable person in the same position. Claims of ignorance or naivety does not constitute defense. Additional monitoring and investigation of transactions should be performed prior to submitting a SAR.

When to report?

24. **To decide should be reported to compliance officer;**

(a) Knowledge or suspicion of criminal activity resulting in someone benefitting

(b) Being aware of an activity so unusual or lacking in normal commercial rationale that it causes a suspicion of money laundering

(c) Knowing or suspecting a person or persons of being involved in crime, or having information that might assist in identifying them

(d) Knowing who might have received the benefit of the criminal activity, or where the criminal property might be located, or getting any information which might allow the property to be located

(e) Thinking that the person(s) involved in the activity knew or suspected that the activity was criminal

(f) Being able to explain suspicions coherently

25. **To decide should be reported to FIU by compliance officer**

(a) Knowing or having reasonable grounds to suspect that another person is engaged in ML; and

(b) Information or other matter giving rise to the knowledge or suspicion come to in a disclosure made under the law?

(c) Knowing the name of the other person or the whereabouts of any laundered property from the disclosure; or

(d) Being able to identify the other person or the whereabouts of any laundered property from information or other matter contained in the disclosure; or

(e) Believing, or being reasonable to believe, that the information or other matter contained in the disclosure will or may assist in identifying the other person or the whereabouts of any laundered property

(f) Being able to apply the professional privileged circumstances exemption apply

(g) Requiring consent

Steps to be taken even if a report has not been submitted to FIU

26. (a) The firm should document decisions related to investigations of unusual activity.

(b) Records should be maintained as required by law, for at least five years from the date when the firm's relationship with the client was terminated or a transaction was completed. If an ongoing investigation is occurring, relevant CDD records should not be destroyed merely because the record retention period has expired.

(c) The firm should determine the actual risk presented by a customer and take appropriate measures to mitigate the risk.

(d) The firm should have sufficient controls and monitoring systems for the timely detection and reporting of potentially suspicious activity and large transaction reporting.

(e) The firm should perform proper due diligence and employees should monitor the activity that may be inconsistent with a customer's source of income or regular business activities.

(f) A firm's system for identifying, monitoring and reporting suspicious activity should be risk–based by directing additional resources at those areas the obliged entity has identified as higher risk such as the firm's size, the nature of its business, its location, the frequency and size of transactions and the types and geographical location of its customers.

Reporting Suspicious Matters

27. It is the employee's responsibility to decide whether to submit an internal report, i.e. to report the incidence to compliance officer. At the same time, compliance officer's responsibility is to decide whether the information reported internally needs to be reported to FIU.

28. Financial Intelligence Unit has been created an electronic reporting system in order to be fast and smooth in submission and receiving process. The system aims to operate efficiently and automatically the reporting and analyzing functions by using modernized technology. Reporting organization needs to have the reporting software and reporting entity code from FIU. And the reporting organization has to

install it into the designated computer by following the instructions and submit the report by using it. FIU would explain the procedure to use reporting software while issuing the software.

29. Financial Intelligence Unit is issuing the guidance note on reporting obligations and evaluation report on the report it received in order to improve the quality of reports, and holding the regular meetings, discussing time by time through telephone, fax phone, email in order to enhance cooperation among Financial Intelligence Unit, Competent Authorities and reporting organizations.

Protection to Whom report to FIU

30. There are some specific provisions to protect to whom report to FIU in the Anti–Money Laundering Law. In section 59(a) of the Law, it expressed that no prosecution and taking action by criminal, civil, disciplinary or administrative means on reporting organizations or their directors, officers or staff who submit reports or provide information in good faith in accord with the provisions of this Law for the breach of the provisions of banking, professional secrecy and agreement. And in section 59(b) of the law, it also stated that the provisions of this law shall prevail the provisions of financial and professional secrecy and confidentiality to be followed by the reporting organizations or their directors, officials or staff. So, those provisions protect to who report to FIU by Law.

Tipping Off

31. 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 FIU;

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

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

32. 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.

33. Regarding to information security, section 66 of the Law described that the person who is serving or served in the Central Body, Financial Intelligence Unit, the

Competent Authority, Reporting Organizations and other government departments and such organizations implementing this Law shall keep of secret any information received within his duty period until the termination of duty, and every responsible person may use the information in accord with the provision of this Law or under the order of a court. It shall be taken action by the Official Secrets Act if this provision is violated. Therefore the persons who have to handle the information including Financial Intelligence Unit, Competent Authorities and reporting organizations is responsible not to be tipping off.

34. But there is a provision to disclosure such information in section 33 of the Law. It is that responsible persons of government departments and organizations or reporting organizations shall not disclose any report or relevant information and any measure under section 32 to any person other than among employees and legal counsel. So it can discuss and inquiry among the employees for the purpose of reporting process.

Penalties in case of Failing to report

35. According to section 46 of the Anti–Money Laundering Law , any responsible person from the reporting organization, in reporting to Financial Intelligence Unit under section 32, presents false statement or conceals facts shall, on conviction, be punished with imprisonment from a minimum of three years to a maximum of seven years and may also be liable to a fine. If the offender is a company or an organization, a fine which may extend to three hundred million kyats shall be imposed on such company or organization. And then at section 48 of the Law, it is described that whoever fails to comply with prohibitory orders and directives relating to money and property issued to him during the investigation period under this Law shall, on conviction, be punished with imprisonment for a term not exceeding seven years and may also be liable to a fine. If the offender is a company or an organization, a fine which may extend to three hundred million kyats shall be imposed on such company or organization. So, reporting organization should note that it would be punished by section 46 and 48 of the Law for failing to report to FIU.

The Address of Financial Intelligence Unit

36. The address is Financial Intelligence Unit Office, Kyun Shwe Myaing St, 1000 Acres (near Ingyin Market), Danatheiddhi Quarter, Zabuthiri Township, Nay Pyi Taw.

Telephone numbers are 067–3421761, 067–3421756, and Fax Mail No. is 067–3421761. Email address is mfiu.str1@gmail.com.

37. Section 18 of the Law expressed that reporting organizations shall carry out the risk assessment of money laundering and financing of terrorism according to the information provided by the Central Body in accord with sub–section (a) of section 8. The risk assessment and any underlying evidence and information shall be recorded in writing, be kept up–to–date and be readily available to the relevant authorities. And section 10(f) of the Law also stated that Financial Intelligence Unit may request the relevant reporting organizations, by limiting a period, to send necessary new information in designated forms for enabling to carry out the functions and duties of the Unit systematically. Again section 10(g) of the law described that Financial Intelligence Unit is entitled to access any report or information received and maintained by reporting organizations, implementing organizations and other government departments and organizations;

Conclusion

39. In conclusion the reporting organizations should strongly cooperate in effort to fight money laundering by reporting suspicious financial transactions and suspicious financial activities to Financial Intelligence Unit, and by supporting extra information when FIU make request to it.

40. These guideline will be reviewed on a periodic basic to be more effective and efficient in practice in order to explain more detail and to add some extra information if it is necessary.

Police Brigadier General Kyaw Win Thein
The Head of Financial Intelligence Unit

Ref. No. 4236 (213)/14–01/ G 4

Date. 26th November 2019

Distribution

Reporting Organizations

Competent Authorities