ROYAL MONETARY AUTHORITY OF BHUTAN

s

Guideline on Anti Money Laundering and Countering of Financing of Terrorism for Capital Market Intermediaries 2021

1. INTRODUCTION

1.1 This guideline is issued in pursuant to Section 45 of the Anti-Money Laundering and Countering of Financing of Terrorism (AML/CFT) Act of Bhutan 2018 or amendment thereof.

1.2 This guideline shall be cited as the ***Anti-Money Laundering and Countering of Financing of Terrorism guidelines for Capital Market Intermediaries (CMIs) 2021.***

1.3 In addition, the Capital Market Intermediaries (CMIs) shall comply with the Anti-Money Laundering and Countering of Financing of Terrorism (AML/CFT) Rules and Regulations 2018 or amendment thereof.

2. GENERAL DESCRIPTION OF MONEY LAUNDERING AND FINANCING OF TERRORISM

2.1 Money laundering is the processing of the proceeds of crime to disguise their illegal origin. Once these proceeds are successfully 'laundered', a person is able to enjoy these funds without revealing the original source. Money laundering can take place in various ways.

2.2 Money laundering is often considered to be associated with the activities of banks and money changers. However, financial institutions, both banks and non- banks, including capital market intermediaries, are susceptible to money laundering activities. Whilst the traditional capital market investment does offer a vital laundering mechanism, particularly in the initial conversion of cash to stock. Capital market investments schemes are one of the most attractive vehicles to the launderer.

2.3 Financing of terrorism is defined as the willful provision or collection, by any means, directly or indirectly, of funds with the intention that the funds will be used, or in the knowledge that they are to be used, to facilitate or carry out terrorist acts. Terrorism can be funded from legitimate income.

3. VULNERABILITIES ASSOCIATED WITH PARTICULAR TYPES OF SECURITIES PRODUCTS

The securities products can be utilized in the layering and integration stages of money laundering once illicit assets are placed in the financial system. However, the securities industry is relatively inhospitable to the placement of illicit assets into the financial system. Nevertheless, certain securities products do pose identifiable ML/TF vulnerabilities even at the placement stage. As in Bhutan, illicit proceeds may directly be placed for buying securities.

The complexity of the securities sector and the variety of intermediary roles involved highlight that no one-size-fits-all AML/CFT approach should be applied. However, this variety and complexity highlights the importance of securities providers' understanding of how their business arrangements raise ML/TF risks both directly (e.g., through transactions executed by customers) and indirectly (e.g., risks associated with the underlying customers of the securities provider's customers, or risks associated with the possibility that an intermediary or other entity on which the securities provider relies to perform a task fails to do so). Securities providers shall implement risk-sensitive measures to mitigate the ML/TF risk faced by them.

This section focuses on the vulnerabilities of some specific types of securities products that may pose significant risk of ML/TF.

3.1 Broker- dealers

One of the most active participants in the securities market is the brokers or dealers in securities. A broker typically acts as an agent for an investor, and enters the securities markets on behalf of an investor to buy or sell a security. In this buying and selling process, some dealers provide liquidity to the capital market by its own capacity of buying and selling. A specific vulnerability associated with broker-dealers is their reliance on another financial institution's CDD process. A broker-dealer might assume that, because another reporting entity has opened an account for a Customer, so the Customer does not pose ML/TF risks for them. The CDD vulnerability is most problematic in relation to the funding of a securities account. If illicit assets are successfully placed at a depository institution, the broker-dealer may assume that, because the funds are from an institution which is subject to AML/CFT rules, the Customer does not pose a ML/TF risk and therefore will accept cheques from that institution to fund a securities account. Once a securities account is funded, a Customer can engage in a number of transactions that further conceal the source of his or her illicit funds, thereby successfully layering and integrating illicit assets that were placed through a depository institution. Important note is that; it is the responsibility of each institution to ensure that the proper CDD process has been completed.

3.2 Asset Managers, Custodians, and Portfolio Managers

Brokers and dealers in securities can be distinguished from those securities intermediaries that are regulated as asset managers, custodian and portfolio managers. The role of a broker and a dealer are clearly delineated from those of custodian or managers. In fact, different registration and regulatory standards may apply for them. Nonetheless, functions can be housed in the same entity by means of multiple registrations. Such advisory functions and broker-dealer functions may be conducted under the same registration. Role of the asset manager, custodian and portfolio manager is generally to advise on the composition of an investment portfolio or to hold securities of local or foreign customers or to manage the contents of investment accounts for retail or institutional Customers respectively. Portfolio management typically involves the provision of financial services in a managed relationship with Customers who are often of high net worth. The value and complexity of products offered to high-net-worth customers, together with the international nature of the business, make the provision of wealth management services potentially attractive to money launderers, to disguise their illicit assets. The custodian services, regardless of the nationality of an investor, has the same potential to be a money launderer as portfolio management and asset management services.

3.3 Shell Companies

The term "shell company" often refers to a non-publicly traded corporation or limited liability company that might have no physical presence and generates little or no independent economic value. These companies are commonly organized in a way that makes their ownership and transaction information easier to conceal. Thus, transactions involving shell companies present a high ML/TF vulnerability. Whilst publicly traded shell companies can be used for illicit purposes, ML/TF vulnerabilities associated with shell companies are heightened when the company is privately held, such that beneficial ownership can be more readily obscured. For example, a domestic or international shell company securities account can be used to evade CDD investigations regarding the beneficial owners of certain assets. In particular, individuals or entities in high-risk areas/jurisdictions or conflict zones can disguise their true identities through a series of shell companies located in various jurisdictions to participate in a financial system that they otherwise would not be able to access. Shell companies can also be used to introduce illicit funds into a financial system and/or generate illicit funds through manipulative or fraudulent securities activities. For example, a brokerage account can be opened in the name of shell

companies and used to engage in fraudulent conduct with regard to low priced, illiquid, low volume or privately placed securities. In addition, a shell company can be established to accept payments from criminal organizations for non-existent services. These payments, which appear legitimate, can be deposited into depository or brokerage accounts and used to purchase securities products that are easily transferable or redeemable.

3.4 Cheques

Cheques can be used to fund securities accounts with a securities intermediary. In addition, the use of cheques is not limited to those drawn from a depository account, but also can involve pay order/bank draft. Money launderers can purchase pay orders/bank draft, pay order with cash over a period of time or through a series of transactions in order to avoid threshold currency reporting requirements. These cheques can then be deposited into securities accounts until a desired amount is reached and used to purchase a security, which is then sold or transferred. Cheques from a depository account also present ML/TF vulnerability because they may unreasonably affect the securities intermediary's risk analysis, in particular with respect to CDD obligations. For example, if a cheque originates from another reporting entity subject to an AML/CFT regulatory regime, a securities firm may not conduct a thorough CDD investigation because it believes that the originating reporting entity has already conducted its own CDD investigation, or because the firm perceives a reduced risk because the customer was able to open an account at another financial institution. This vulnerability can become systemic if numerous securities intermediaries perceive a reduced risk based on the activities of others. In addition, even if the reporting entity from which the cheque originated has conducted thorough CDD and not detected anything suspicious, there may still be an ML/TF risk that the securities intermediary, through its own knowledge of the investor, may be in a unique position to identify. In particular, CDD not only involves mere customer identification but establishing the purpose and intended nature of the business relationship.

3.5 Short Selling

In the securities industry short selling generally involves the practice of selling securities that are not actually owned by the seller, or that will be borrowed for delivery. In a "naked" short sale, the seller does not borrow or arrange to borrow the securities in time to make delivery to the buyer within the standard settlement period. The investment strategy behind short selling is the hope that a profit will be made from the difference in price of the assets sold and those purchased (at a lower price) for return to the borrower. Short selling (where not approved) is a trading vehicle that can be linked to market manipulation or insider trading, which are both predicate offences that could be the basis for ML/TF.

3.6 Insider Trading

Insider trading involves situations where the person who buys and sells securities, whether a company insider or not, does so in violation of a fiduciary duty or other relationship of trust and confidence, while in possession of material, non-public information about the security. This includes situations where a person in possession of material, non-public information provides this information to someone else for trading where, depending on the circumstances, the recipient of the information can violate insider trading laws as well. Insider trading is unique to the securities industry and generates illicit assets. As a predicate offence for money laundering (to be included later on) this type of misconduct is reportable as STR. The illicit assets generated by insider trading can be laundered through the securities industry itself or through other parts of the financial sector. The most common example of laundering would be the simple transfer of illicit proceeds to a bank account.

3.7 Market Manipulation

Market manipulation generally refers to conduct that is intended to deceive investors by controlling or artificially affecting the market for a security. In particular, the manipulator's purpose is to drive the price of a security up or down in order to profit from price differentials. There are a number of methods that manipulators use to achieve these results. The most pervasive market manipulation method involves what is referred to as a "pump-and-dump" scheme. This scheme involves touting a company's stock with false or misleading statements, often in conjunction with securities trades that raise the price of the security or make it appear as if the securities trading volume is higher than it actually is. Therefore, the security price is artificially raised ("pumped"); the security is then sold ("dumped") for a profit. Often the underlying security is low priced, illiquid, and trades with little volume. Another most used method is circular trading. In this mechanism a group of syndicated persons manipulate share price by buying and selling of shares at their own from different corners at their predetermined price.

3.8 Securities Fraud

Securities frauds broadly refer to deceptive practices in connection with the buy and sale of securities. In this regard, securities fraud encompasses insider trading and market manipulation activities and poses significant ML/TF risks for the CMIs.

4. GENERAL PRINCIPLES AND POLICIES TO COMBAT MONEY LAUNDERING AND TERRORISM FINANCING

4.1 A reporting entity is required to take the necessary steps in order to prevent ML/TF and shall have a system in place for reporting suspected ML/TF transactions to FID.

4.2 In countering ML/TF, a reporting entity shall ensure the following:

a) **Establishing internal controls:** A reporting entity shall develop and adopt programs and policies which are consistent with the principles set out under the AML/CFT Act 2018, AML/CFT Rules & Regulations 2018 and these Guidelines. This program shall be approved in writing by the board directors of the company which carries out the business of broker/dealer/market intermediary.
b) **Compliance with laws:** A reporting entity shall ensure that laws and regulations are adhered to, that business is conducted in conformity with high ethical standards, and that service is not provided where there is good reason to suppose that transactions are associated with ML/TF activities.
c) **Training Programme**: A reporting entity must also ensure ongoing training programs are conducted to keep its board of directors and employees abreast on matters under the AML/CFT Act, AML/CFT Rules & regulations and this Guidelines.
d) **Risk-based approach:** A reporting entity shall ensure that the depth and breadth of its policies and procedures to identify, assess, monitor, manage and mitigate ML/TF risks commensurate with the nature, scale and complexity of its activities.
e) **Customer Due Diligence:** A reporting entity must have an effective procedure to identify its customers and to obtain satisfactory evidence to verify its customers' identity.

4.3 The board of directors shall ensure that the reporting entity regularly reviews its policies, procedures and controls to ensure that they are effective and in line with the international standards, particularly the FATF Recommendations on countering ML/TF.

5. RISK-BASED APPROACH APPLICATION

The reporting entity in pursuant to **Section 51 of the AML/CFT Act of Bhutan 2018** shall establish a risk-based approach (RBA) to prevent and detect ML and TF. The RBA is expected to identify, assess, and understand the ML/TF risks facing CMIs and take AML/CFT measures commensurate with those risks in order to mitigate them effectively. It provides an assessment of the threats and vulnerabilities of the reporting institution from being used as a conduit for ML/TF. The RBA process shall be dynamic, with risk assessments and mitigation measures being updated on an on-going basis.

In formulating policies and procedures for the prevention of ML/TF, a reporting entity must take appropriate steps to identify, assess, and mitigate its ML/TF risks. **Section 59-61 PART V of the AML/CFT Rules & Regulation 2018** provides the measures to be adopted in implementing a risk-based approach.

5.1 Risk assessment and profiling

5.1.1 The assessment and profiling processes shall incorporate the following:

- **a)** Documenting the reporting entity risk assessments and findings;
- **b)** Considering all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied;
- **c)** Keeping the reporting entity risk assessment up-to-date taking into account changes in surrounding circumstances affecting the reporting entity;
- **d)** Shall have a scheduled periodic assessment or as and when directed by the FID; and
- **e)** Shall have appropriate mechanisms to provide risk assessment information to the FID.

5.1.2 A reporting entity is also required to identify and assess the ML/TF risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products. The reporting entity shall undertake risk assessments prior to the launch or use of such products, practices and technologies and take appropriate measures to manage and mitigate such risks.

5.1.3 In assessing the level of risk of a customer from a particular country, a reporting entity shall assess the standards of prevention of ML/TF in that country based on the reporting entity's knowledge, experience and other reliable sources of that country. The higher the risk, the greater the due diligence measures that should be applied when undertaking business with the customer from that country.

5.1.4 A reporting entity is required to also implement and maintain appropriate policies and procedures to conduct risk profiling of their customer during the establishment of the business relationship. In determining the risk profile of a particular customer, the reporting entity shall take into account, among others the following factors

- **a.** Customer risks e.g. residents or non-residents, occasional or one off, natural or legal person;
- **b.** Geographical location of business or country of origin of customers;
- **c.** Products or services;
- **d.** Transactions or distribution channel e.g. cash-based, face-to-face or non-face-to-face or cross-border; and
- **e.** Any other information suggesting that the customer is of higher risks

5.2 Risk management and mitigation

A reporting entity is required to:

a) Have policies, procedures and controls, which are approved by the board of directors, to enable it to manage and mitigate effectively the ML/TF risks that have been identified;
b) Monitor the implementation of those policies, procedures and controls and to enhance them if necessary; and
c) Take enhanced measures from time to time.

5.3 AML/CFT Program

5.3.1 A reporting entity shall provide to the FID a copy of its AML/CFT Program within 3 months of the commencement of these guidelines and within one month of any review of the program conducted in accordance with sub-regulation **7.4 of this guideline.**

5.3.2 A reporting entity shall conduct review on the AML and CFT programs on the basis of risk or when significant changes are made to their business or when any previous review is out of date. The FID/supervisor shall be notified upon completing an assessment of their ML and TF risks or a review of any such assessment.

6. CUSTOMER DUE DILIGENCE (CDD)

6.1 CDD at the Point of Establishing Business Relationship

6.1.1 The reporting entity must obtain sufficient evidence of the identity of any customer as soon as reasonably practicable after it has contact with a customer.

6.1.2 The reporting entity has a responsibility for verifying the identity of the investor, and the beneficial owner of the investor. The verification should provide a reasonable basis for an institution to believe that the true identity of the investor is adequately known.

6.1.3 A reporting entity must put in place appropriate risk-based systems and controls to determine whether and in what circumstances KYC information should be updated or verified in respect of its customers for ongoing customer due diligence purposes.

6.1.4 The identity verification procedures of an institution may be risk-based depending on the type of investor, business relationship, or transaction. Where there are low risks, it may be appropriate for an institution to apply simplified verification procedures. These procedures, of course, must still be sufficient for the institution to achieve the goal of verification – establishing a reasonable belief that it knows the true identity of its investor.

6.1.5 Prior to providing a financial service to a customer a reporting entity shall obtain the identification documentation as per Section 107 & 108, Part VI of the AML/CFT Rules & Regulations 2018, and record the specified information in relation to that customer and retain a copy of the documents as per Section 67 & 68 of the AML/CFT Act 2018.

6.1.6 A customer who fails to provide evidence of his identity shall not be allowed to engage in business relations with the reporting institution. Additional measures shall be undertaken to determine whether to proceed with the business relationship, where initial checks failed to identify the customer or give rise to suspicions that the information provided is false.

6.2 On-Going Customer Due Diligence

The reporting entity shall conduct on-going due diligence on the business transactions with the customer to ensure that the transaction are consistent with the firm's knowledge of customer's business risk and source of income as per Section 69 of the AML/CFT Rules & Regulations 2018.

6.3 Reporting Obligations

Pursuant to Section 145, Part VII of the AML/CFT Rules & Regulations 2018 the reporting entity shall report STRs, CTRs and any other reports to the FID. This guideline establishes the specific reporting obligations.

6.3.1 Reporting cash and other transaction

Where an obligation to lodge a CTR (taken place within a month) arises the report shall be delivered to the FID within the 10th day of the succeeding month.

All the trading transaction, high value transaction, multiple trading transactions done in cash/ Cheque/ draft (**no threshold limit**) shall be reported to the FID on a monthly basis in the required format via *BFIAS portal* as per Section 153-160 of the AML/CFT Rules & Regulations 2018.

6.3.2 Suspicious transaction reporting obligation

a) The reporting entity shall report to the FID any transaction or attempted transaction which the firm has reasonable suspicion that it may relate to the commission of any unlawful activity in terms of Section 146-152 of the AML/CFT Rules & Regulations 2018.

b) A reporting entity is required to report all suspicious transactions, including attempted transactions, regardless of the amount of the transaction. A reporting entity should be aware that in some cases, suspicion may be formed after a considerable time from the date of the transaction, in view of subsequent additional information.

c) The reporting entity shall lodge with the FID a suspicious transaction report (STR) in the required format via BFIAS portal or other mechanism as deemed required by FID. Where an obligation to lodge a STR arises the report shall be made no later than two working after the transaction or attempted transaction has taken place.

d) Refer to *Suspicious Transaction Guidelines for Reporting Entities 2019* for some examples of suspicious transactions. The list is non- exhaustive and only provides examples of ways in which money may be laundered through the capital market.

7. APPOINTMENT OF AML/CFT COMPLIANCE OFFICER (AMCLO)

The companies shall designate an AML/CFT Compliance Officer (AMLCO) with reference to Section 71-77 of the AML/CFT Rules & Regulations 2018**.**

8. DELIVERY OF REPORTS

8.1 Reporting entities are required to ensure that the designated branch or subsidiary AMLCO is responsible for channeling all internal suspicious transaction reports received from the employees of the respective branch or subsidiary to the AMLCO at the head office. In the case of employees at the head office, such internal suspicious transaction reports shall be channeled directly to the AMLCO.

8.2 Reporting entities are required to have in place policies on the duration upon which internally generated suspicious transaction reports must be reviewed by the AMLCO, including the circumstances when the time frame can be exceeded, where necessary.

8.3 Upon receiving any internal suspicious transaction report whether from the head office, branch or subsidiary, the AMLCO must evaluate the grounds for suspicion. Once the suspicion is confirmed, the AMLCO must promptly submit the suspicious transaction report. In the case where the Compliance Officer decides that there are no reasonable grounds for suspicion, the Compliance Officer must document and file the decision, supported by the relevant documents.

8.4 Reports required to be delivered to the FID shall be via *BFIAS portal* or any other mechanism as deemed required by FID. The reporting entity is responsible for ensuring that the reports are delivered within the time required by this guideline.

9.PROVISION OF ADDITIONAL INFORMATION

If a reporting entity has communicated information to the FID, the FID may, by written notice given to the reporting entity, require the reporting entity to give such further information as is specified in the notice, within the period and in the manner specified in the notice, to the extent to which the reporting entity has that information; or to produce, within the period and in the manner specified in the notice, such documents as specified in the notice; and relevant to the matter to which the communication relates.

10. INTERNAL CONTROL/AUDIT

In pursuant to Section 54 of AML/CFT Act 2018, the reporting entity shall ensure that effective internal controls are in place by establishing appropriate procedures and ensuring their effective implementation. The internal audit and compliance functions have an important role in evaluating and ensuring adherence to the AML/CFT policies and procedures. The procedures shall cover proper management oversight systems and controls, segregation of duties, training and other related matters. Responsibility shall be explicitly allocated and that the auditor has direct access and reports directly to management and the board of directors to ensure that the AML/CFT policies and procedures are implemented effectively.

11. RECORD KEEPING

For Record keeping requirements, the reporting entity shall retain record for a minimum period of five years in pursuant to Section 97-99 of the AML/CFT Rules & Regulation 2018.

12. CONFIDENTIALITY AND PROTECTION OF INFORMATION

For Confidentiality and Tipping off provisions, the reporting entity shall refer to Section 76-79 of AML/CFT Rules & Regulation 2018.

13. PENALTY

Non-compliance of any provision of this guideline shall be liable to a fine as per Part XVIII of AML/CFT Rules & Regulation 2018.