ROYAL MONETARY AUTHORITY OF BHUTAN

FIU G4: Guideline on Anti Money Laundering and Combating the Financing of Terrorism for Capital Market Intermediaries 2014

1. INTRODUCTION

1.1) This guideline is issued pursuant to Section 141(g) and Section 210 of the Financial Service Act (FSA) 2011. This guideline must be read in conjunction with the additional requirements under the Financial Services Act, 2011.

1.2) This guideline may be cited as the ***Anti-money Laundering and Combating the Financing of Terrorism guidelines for Capital Market Intermediaries 2014.***

1.3) In addition the reporting entities are also to comply with the relevant sections of the FSA 2011 and the Anti-Money Laundering and Combating the Financing of Terrorism Regulations 2015.

2. 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' the criminal is able to enjoy these monies without revealing their original source. Money laundering can take place in various ways.

2.2). Financing of terrorism can be defined as the willful provision or collection, by any means, directly or indirectly, of funds with the intention that the funds should 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.

2.3). Money laundering is often thought to be associated solely with banks and moneychangers. But in reality financial institutions, both banks and non- banks, including capital market intermediaries, are susceptible to money laundering activities. Whilst the traditional capital market investment do 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.

3. VULNERABILITIES ASSOCIATED WITH PARTICULAR TYPES OF SECURITES PRODUCTS

3.1 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 proceed may directly be placed for buying securities. This section focuses on the vulnerabilities of some specific types of securities products that may pose significant risk of ML/TF.

3.2 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 financial institution has opened an account for a Client, so the Client 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 Client 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 Client 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 proper CDD process has been completed.

3.3 Asset Managers, Custodian and Portfolio Managers.

Brokers and dealers in securities can be distinguished from those securities intermediaries that are regulated as asset manager, 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 clients or to manage the contents of investment accounts for retail or institutional Clients respectively. Portfolio management typically involves the provision of financial services in a managed relationship with Clients who are often of high net worth. The value and complexity of products offered to high net worth Clients, 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 same potential to money launderer as portfolio management and asset management services.

3.4 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.

3.5 Cheques can be used to fund securities account 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 financial institution subject to an AML/CFT regulatory regime, a securities firm may not conduct a thorough CDD investigation because it believes that the originating financial institution has already conducted its own CDD investigation, or because the firm perceives a reduced risk because the client 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 financial institution 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 Client identification but establishing the purpose and intended nature of the business relationship.

3.6 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.

3.7 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.

3.8 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 share at their own from different corner at their predetermined price.

3.9 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 CMI.

4. AML/CFT PROGRAM

The reporting entity should develop and implement a written program reasonably designed to prevent it from being used for money laundering and terrorist financing. This program should be approved in writing by the directors of the company which carries out the business of broker/dealer/market intermediary or by the trustee/s of a unit trust. An AML/CFT program which should, at a minimum, should cover:

- CDD, the detection of unusual or suspicious transactions and the reporting obligation, and the communication of these policies, procedures and controls to the employees,
- appropriate compliance management arrangements,
- record keeping arrangements,
- an ongoing employee training programme, and
- an adequately resourced and independent audit function to test compliance (e.g. through sample testing) with these policies, procedures, and controls

4.1 Provision copies to RMA

A reporting entity must provide to the RMA 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 4.2 of this guideline.

4.2 Review of programs

A reporting entity must conduct a review of its AML CFT Program within two years of the lodgment of its AML CFT Program and within every two years thereafter.

4.3 Compliance Report

A reporting entity shall provide to the RMA every six months a report on the actions taken by it to give effect to its AML CFT Program.

5. CUSTOMER IDENTIFICATION PROCEDURES AND KNOW YOUR CUSTOMER (KYC) REQUIREMENTS

5.1 The broker/dealer firm/market intermediary must obtain sufficient evidence of the identity of any client as soon as reasonably practicable after it has contact with a client.

5.2 The broker/dealer firm/market intermediary 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.

5.3 A broker/dealer firm/market intermediary 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.

5.4 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.

5.6 Prior to providing a financial service to a customer a reporting entity shall sight the identification documentation as per section **4.3 of the AML/CFT Regulation 2015**, and record the specified information in relation to that customer and retain a copy of the documents as required under section **16.1 of AML/CFT Regulations 2015.**

6. THE MANDATORY RULES ON KYC/CDD include the following sections:

6.1. CUSTOMER DUE DILLIGENCE

Every broker/dealer firm/market intermediary (as a reporting entity) shall conduct on-going due diligence on the business transactions with the customer to ensure that the transaction are consistence with the firm's knowledge of customer's business risk and source of income as per section 4.11 of the AML/CFT Regulations 2015.

6.2. REPORTING OBLIGATION

The Financial Services Act 2011, Section 141 (a), provides for reporting entities to report both STRs and CTRs to the FIU. This guideline establishes the specific reporting obligations.

6.2. 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 FIU within 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 FIU on a monthly basis, in the format and requirement as per letter no RMA/FIU/2013/1486 dated 22nd October 2013 (see Annex A,)

6.2.2 Suspicious transaction reporting obligation

Every broker/dealer firm/market intermediary shall report to the Financial Intelligence Unit:-
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 6.1 of the AML/CFT Regulations 2015.

The reporting entity shall lodge with the FIU a suspicious transaction report (STR) in the required format as specified in Annex B.

Where an obligation to lodge a STR arises the report shall be delivered to the FIU no later than 2 working days on being satisfied that the transaction is suspicious.

7. DELIVERY OF REPORTS TO FIU

Reports required to be delivered to the FIU under these guidelines may be delivered by post, by hand or electronically. The time limits apply irrespective of the delivery method used by the reporting entity. The reporting entity is responsible for ensuring that the reports are delivered to the FIU within the time required by this guideline. In urgent cases the reporting entity should notify the FIU of the details of the transaction by telephone and send the report by post, hand or electronically in accordance with this guideline. Refer **section 6.1.5-6.1.13 of AML/CFT Regulation 2015** for details.

8. PROVISION OF ADDITIONAL INFORMATION

If a reporting entity has communicated information to the FIU, the FIU 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.

9. INTERNAL CONTROL/AUDIT

Internal audit/inspection departments of the concerned reporting entities companies should verify on a regular basis, compliance with policies, procedures and controls relating to money laundering activities. It is of importance that the audit function is independent and, if applicable, that the auditor has direct access and reports directly to management and the board of directors. The reports should specifically comment on the robustness of the internal policies and processes in this regard and make constructive suggestions where necessary, to strengthen the policy and implementation aspects.

10. RECORD KEEPING

For Record keeping requirement please refer section 16 of AML/CFT Regulation 2015.

11. APPOINTMENT OF AML/CFT COMPLIANCE OFFICER

11.1. The companies should designate an AML/CFT Compliance Officer under **FIU G1: Guidelines for appointment of AML/CFT Compliance Officer (AMLCO**). The name of the principal compliance officer should be communicated to FIU immediately. The compliance officer should be well versed in the different types of products and transactions which the institution handles and which may give rise to opportunities for money laundering and the financing of terrorism.

12. CONFIDENTIALITY AND PROTECTION OF INFORMATION

For Confidentiality and Tipping off provisions reporting entity should refer section 22 of AML/CFT Regulation 2015.

13. PENALTY

Non compliance to any provision of this guideline shall be liable to a fine as per **section 23 of AML/CFT Regulation 2015.**