SME-Development Bank

Anti-Money Laundering and Combating of Terrorist Financing Policies & Procedures

SME-Development Bank Limited

Anti-Money Laundering & Combating of Terrorist Financing Policies & Procedures

1. Compliance Responsibilities

The bank actively participates in the campaign against money laundering and terrorist financing launched by the government. It strictly follows the instructions on anti-money laundering measures laid down by the Central Control Board (CCB) and the Central Bank of Myanmar (CBM).

The bank has given necessary instructions to its branch and department managers to be able to fully comply with the Control of Money laundering Laws and Rules enacted by the government and related instructions and guidelines laid down by the Central Bank of Myanmar. The bank keeps the Control of Money Laundering Law and Rules, instructions from the Central Bank of Myanmar and 40+9 Recommendations of FATF as guidelines for AML requirements.

It has formed an Anti-Money Laundering and Compliance Unit headed by a senior general manager and other senior officials of the bank as members to comply with the law, rules and instructions.

The manager of each and every branch is designated as a compliance officer and a compliance team is formed with his or her deputies as members.

The compliance teams thoroughly check every transaction daily and they send reports on STRs and CTRs to CCB and CBM without any delay on the same day.

The teams send their monthly reports to the Anti-Money Laundering and Compliance Unit at the head office.

The bank cooperates with law enforcement agencies such as Financial Intelligence Unit (FIU) and CBM in anti-money laundering and combating terrorist financing.

The bank issues necessary instructions on AML/CFT to be followed by its staff members.

It always tries to increase awareness of AML/CFT both within the compliance teams and among the employees of the bank irrespective of ranks.

2. Customer Due Diligence/Know Your Customer Procedures

Bank officials have to undertake CDD measures and KYC procedures according to FATF Recommendations and AML Laws and Regulations.

Bank tries to verify the status and identities of prospective customers before business relation is established: in the case of opening a new account, bank gets customer's identifications such as photo copy of the customer's national registration card, his address and contact number together with proper introduction of two account holders of the bank. When remitting money from one bank to another, bank also takes identities of both drawer and drawee: names, ID numbers, addresses, contact numbers and reason of remitting the money. And it is the duty of members of the bank staff to try to know their customers: who they are and what they are. The bank staff does not allow opening of anonymous and fictitious accounts with the bank.

In the case of companies, bank gets necessary information for opening a new account: certificate of incorporation, memorandum and article of association, list of board of directors and its resolution to open an account with the bank, list of shareholders etc.

Bank officials constantly keep in touch with their customers and are urged to update their information on customers. The bank carefully and properly keeps track records of all customers' accounts. It promotes its customer due diligence by differentiating between regular and walk-in customers.

3. Reporting CTR and STR

The compliance team of a branch has to report to CBM and CCB on CTR if the amount of transaction reaches the threshold amount set by the central bank and on STR if the compliance team is convinced that the transaction is suspicious. The compliance team uses the following check-list prescribed by the central bank in determining whether a transaction is suspicious or not:

1. Transferring deposit-money to another bank in the same town within a short time.
2. The names of the transferor and the transferee are similar.
3. Providing insufficient or incorrect information when opening a bank account
4. Declining to provide complete information in filling up forms.
5. A walk-in-customer, who is not a regular customer of the bank, failing or refusing to provide complete information regarding an inland remittance.
6. Withdrawal of proposed bank transactions for lack of information required by the bank.
7. Depositing money too big to reflect the nature of the customer's existing business.
8. A regular customer being suspected of conducting bank transactions for or on behalf or under the direction of a third party.
9. Remitting money not compactable with the business mentioned in the application.
10. A customer depositing funds in a local bank and instructing it to remit funds abroad by TT simultaneously.
11. Remitting funds to countries under surveillance (viz., countries allowing tax exemptions, countries producing/trading in illicit drugs).
12. Depositing money to the one and same account by different persons to avoid report to the authorities regarding deposit of money over and above the set limit.
13. Remitting funds to the one and same account from different places within a short period of time.
14. A regular customer conducting a transaction much larger than his/her usual transaction.
15. Making unusual transactions not commensurate with ordinary business.
16. Suddenly operating a dormant account left unused for some times.
17. Refusal by the customer to reveal the relation between him/her and the transferee.
18. Refusing to answer relevant queries regarding a remittance.
19. A foreigner depositing a large amount of money into a local bank account.
20. Depositing a large amount of money in installments to the one and same account within a short period.
21. Remitting money in installments to different accounts abroad.

In June 2009, the Central Bank of Myanmar added another 15 points to the above list for scrutinizing suspicious transactions. The compliance teams carefully check every bank transaction using the check-lists prescribed by the central bank.

After reporting the CTR and STR to the CCB and CBM, compliance officers of branches have to submit the information to the bank's compliance unit at HQ on monthly basis.

4. Record keeping

The bank keep records of customers records of customers: their identifications, account files, registers, transactions, documents, correspondences etc. for at least five years after the business relationship is ended.

5. Staff Training on AML/CFT

The bank sends its senior officials to training on AML/CFT conducted by me CBM and FIU. Such trainings also include anti-money laundering and combating financing terrorist measures in the syllabus of its in-house training programs.