

# Module 10

## Good Market Practices Identified from AML/CFT Self-Assessment Program

(October 2007)

# Good Market Practices Identified from AML/CFT Self-Assessment Program

This list of good market practices, derived from a survey of the AML/CFT self assessment results of selected LCs in April 2007, is intended to be a practical guide for LCs and AEs to take into account when reviewing the effectiveness of their policies and procedures on prevention of money laundering and terrorist financing. These “good market practices” should not be taken as exhaustive nor superseding or overriding the SFC’s Prevention of Money Laundering and Terrorist Financing Guidance Note.

# Role of senior management/ board of directors in AML/CFT compliance governance issues

- ❖ To accord AML/CFT compliance due priority, senior management may play an active role in the following areas:
  - Endorsing AML/CFT policies.
  - Appointing senior staff responsible for AML/CFT compliance.
  - Approving or declining high risk customers.
  - Approving or declining third party payments.
  - Reviewing suspicious activities/cases identified by the staff.

# Role of senior management/ board of directors in AML/CFT compliance governance issues

- Supporting compliance investigation of suspicious cases.
  - Participating in AML/CFT training.
- ❖ To reinforce the importance of AML/CFT compliance, the board of directors may contribute by:
- Overseeing the implementation of AML/CFT policies as part of their broader governance role.
  - Reviewing reports of violations of AML/CFT procedures and controls.

# AML/CFT policies and procedures

- ❖ To help ensure that appropriate and effective AML/CFT policies and procedures are in place, firms may implement the following steps:
  - AML/CFT policies are endorsed by senior management and effectively communicated to all staff by means of training and utilizing suitable forms of testing to ensure proper understanding of the policies.
  - Appoint a person to regularly review changes to applicable AML/CFT rules and regulations, and where necessary, make changes or updates to ensure compliance.
  - Perform periodic audits or compliance checks of AML/CFT controls, including clients' identification and verification procedures.
  - Issue and distribute AML/CFT internal audit reports or compliance checking reports to all relevant business and functional departments as well as to senior management.

# Customer acceptance and customer due diligence

- ❖ To undertake customer acceptance and due diligence measures on a risk sensitive basis, firms may:
  - (i) *Risk-based assessment*
    - Perform risk-based and extensive know-your-customer assessment in order to ascertain a customer's identity, beneficial owners, nature and background of its business activities and source of funds and apply a risk rating to determine the extent of ongoing monitoring.
    - Categorise customers into distinct risk categories – high, medium and low risk. High risk customers are managed by focused resources and enhanced due diligence processes.

# Customer acceptance and customer due diligence

## *(ii) On-going due diligence*

- Conduct periodic reviews depending on a customer's risk rating. This risk-based approach allows more detailed and enhanced reviews to be conducted for higher risk customers on a more frequent basis than low/medium risk customers.
- Generate reports identifying those accounts showing activity which fulfils predetermined criteria, such as large transaction volume, or increased account usage. The compliance officer would review and decide if the transactions made were consistent with the customer's profile.

# Customer acceptance and customer due diligence

## *(iii) Identification of Politically Exposed Persons (“PEPs”) and related enhanced due diligence*

- Use internet or other web-based tools to perform background screening.
- Employ external databases to perform background screening, including names of customers, directors, shareholders, authorised signatories and beneficial owners and perform batch screening on all accounts regularly.



# Customer acceptance and customer due diligence

- Classify PEPs as high risk customers and adopt enhanced due diligence and escalation processes, for example by
  - Assessing the PEP risk by obtaining information such as the customer's political function, country of origin, type of services and products sought and the source of wealth and funds etc.
  - Seeking senior management's approval before opening PEP accounts.
  - Reviewing transactions of the PEP clients on a periodic basis.

# Recognition and reporting of suspicious transactions

- ❖ To facilitate the identification of suspicious transactions and help ensure that the legal requirements for reporting suspicious transactions to the JFIU and prohibitions against tipping-off are complied with, firms may:
  - (i) *Recognition and reporting of suspicious transactions*
    - Implement automated transaction monitoring system utilising software which is designed to detect patterns of unusual transactions and suspicious transactions.
    - Arrange to have exception reports automatically escalated to the compliance officer for review, approval and, where necessary, to form the basis for further investigation, reporting, raising the risk rating of a customer for enhanced monitoring.

# Recognition and reporting of suspicious transactions

- Review these reports from time to time to ensure that they have been properly updated to incorporate new indicators of suspicious activity.
- Incorporate organisation specific indicators of potentially suspicious or unusual activities into AML/CFT policies and AML/CFT training.
- Conduct background checks using reliable and independent source documents and database before establishing business relationships in order to identify terrorist suspects at the initial account opening stage and on an ongoing basis thereafter.

# Recognition and reporting of suspicious transactions

## *(ii) Cash or third-party payments*

- Require approval of cash or third party payments by Head of Compliance and Head of relevant Business Department.
- Perform regular review on activities such as frequent fund transfers or cheque payments involving unverified or difficult to verify third parties or other unusual fund movements and investigate accounts with unusual activities.

# Recognition and reporting of suspicious transactions

(iii) *No tipping-off*

- Put in place procedures whereby
  - Account executives and other relevant staff receive AML/CFT training and are fully cautioned against tipping off customers and made aware that they are subject to criminal liability for such actions.
  - Only a limited number of persons, e.g. the compliance officer and senior management, are privy to suspicious transaction reports which are made to the JFIU strictly on a need-to-know basis.
  - Account executives are not informed when suspicious transaction reports are made to the JFIU to prevent tipping off.

## Staff training

- ❖ To help ensure that appropriate and effective staff training procedures are in place, firms may:
  - Distribute their internal AML/CFT policies to new staff members during induction training.
  - Require newly recruited staff to complete training on AML/CFT and thereafter refresh themselves on AML/CFT policies and procedures regularly.
  - Incorporate new or updated changes in AML/CFT regulations or policies whenever necessary and inform staff of these changes through different means, e.g. circulation of revised policy, internal circulars or email alerts.



# Staff training

- Provide tailored AML/CFT training for front office employees.
- Utilize suitable forms of testing to ensure proper understanding of the policies, e.g. quizzes.