

# **Seminar for Money Service Operators “To put the Anti-Money Laundering and Counter-Terrorist Financing Policies, Procedures and Controls in place”**



Money Service Supervision Bureau

May 2013



# Disclaimer

- The information contained in this website is provided by the Customs and Excise Department (the Department) for general information and reference only. Whilst the Department will endeavour to ensure the accuracy of the information on this website, the Government of HKSAR and the Department do not guarantee or warrant that such information is accurate. Moreover, the inclusion of hyperlinks to other websites is only to facilitate cross-reference. The Government of HKSAR and the Department expressly state that they have not approved or endorsed the content thereof. Users shall verify information obtained from this website by making reference to other sources when making material decisions. The Government of HKSAR and the Department is not responsible for any loss or damages incurred for any cause whatsoever in relation to or as a result of the use of the information on this website.
- The copyright and all other intellectual property rights in the information on this website belong and are reserved to the relevant owners. The Government of HKSAR and the Department shall not be liable for any loss incurred or damages suffered by any person as a result of any actual or alleged infringement of copyright or other intellectual property rights.

# Policy Statement - Requirement (I)



## AMLO (Schedule 2 Section 23)

- a financial institution (FI) must take all reasonable measures –
  - to ensure that proper safeguards exist to prevent a contravention of any requirement under Part 2 or 3 of the Schedule; and
  - to mitigate money laundering (ML) and terrorist financing (TF) risks

# Policy Statement - Requirement (II)



## AML Guideline (Chapter 2.1)

- to ensure compliance with this requirement, FIs should implement appropriate internal Anti-Money Laundering/Counter-Terrorist Financing policies, procedures and controls (“AML/CFT systems”)

# Policy Statement - Requirement (III)



## FATF (Recommendation 1)

- countries should require FIs to identify, assess and take effective action to mitigate their ML and TF risks.
- FIs should be required to have policies, controls and procedures that enable them to manage and mitigate effectively the risks that have been identified.



# Policy Statement - Purposes

- to provide a framework of direction to the business and its staff to AML/CFT
- to identify named individuals and functions responsible for implementing the policy
- to set out how senior management undertakes its assessment of the risks the company faces and how these risks are to be managed
- to focus the minds of staff on the need to be constantly aware of the risks and how these risks are to be managed



# What should a Policy Statement include? (I)

- the culture and values to be adopted and promoted within the business towards the prevention of ML/TF
- allocation of responsibilities to specific persons
- a summary of the company's approach to assessing and managing its ML and TF risk
- a summary of the company's procedures for carrying out appropriate customer identification and verification, customer due diligence, and monitoring checks on the basis of their risk-based approach



## What should a Policy Statement include? (II)

- a commitment to ensuring all relevant staff are made aware of the law and their obligations under it and are regularly trained in how to recognize suspicious activity / transaction
- recognition of the importance of staff promptly reporting suspicious activity / transaction
- a summary of the appropriate monitoring arrangements in place to ensure that the firm's policies and procedures are being carried out





# Culture and Values



# Culture and Values

- takes all reasonable measures to ensure proper safeguards exist to mitigate the risks of ML and TF
- takes all reasonable measures to prevent a contravention of any requirement under the AMLO and the AML Guideline
- implements adequate and appropriate AML and CFT policies, procedures and controls
- identifies and assesses all the risk factors



# Responsibilities



# Responsibilities

- Senior management
  - assess the risks the firm faces
- Compliance Officer
  - prevent and detect ML/TF
- Money Laundering Reporting Officer
  - report suspicious transactions to the JFIU
- Frontline staff
  - judge whether a transaction is suspicious



# **Risk Identification & Assessment**



# Risk Identification & Assessment (I)

- identify the risks inherent in the industry and faced by this particular business
- establish and implement adequate & appropriate AML/CFT systems taking into account the following risk factors:
  - types of customers and behaviour
  - product / service
  - delivery channels
  - customer's residing country / geographical locations involved



# Risk Identification & Assessment (II)

- Customer Risk
  - customers' businesses handle large amounts of cash
  - customers with complex business ownership structures with the potential to conceal underlying beneficiaries
  - customers who are potential Politically Exposed Persons
  - customers who are not operate local business
  - new customers/customers carrying out large transactions
  - non face-to-face customers
  - source of funds cannot be easily verified

# Risk Identification & Assessment (III)



- Product / Transaction Risk
  - a number of transactions below the amount requiring ID checks carried out by the same customer within a short space of time
  - a number of customers sending payments to the same individual
  - complex or unusually large transactions
  - uncharacteristic transactions which are not in keeping with the customer's known activities





# Risk Identification & Assessment (IV)

- Delivery Channel Risk
  - non face-to-face account opening – sales through online, postal or telephone channels
  - business relationship is indirect – business sold through intermediates

# Risk Identification & Assessment (V)



- Country / Geographical Risk
  - high levels of organized crime
  - increased vulnerabilities to corruption
  - inadequate systems to prevent and detect ML/TF



# Carrying out Customer Due Diligence



# Carrying out Customer Due Diligence (I)

- Circumstances requiring CDD measures
  - at the outset of a business relationship
  - before performing any occasional transaction
    - ◆ aggregate value  $\geq$  \$120,000 or
    - ◆ wire transfer  $\geq$  \$8,000
  - suspicion of ML/TF
  - doubt on the veracity and adequacy of the information previously obtained

(AML Guideline Chapter 4.1.9)



# Carrying out Customer Due Diligence (II)

- Measures of CDD
    - identify & verify identity
      - ◆ customer & beneficial owner
    - identify & verify identity and authority
      - ◆ a person purporting to act on behalf of the customer
    - obtaining information on the purpose & nature of the business relationship
- (AML Guideline Chapter 4.1.3)



# Carrying out Customer Due Diligence (III)

- Identify & verify identity of natural persons (I)
  - collecting the identification information:
    - ◆ full name
    - ◆ date of birth
    - ◆ nationality
    - ◆ identity document type and number



# Carrying out Customer Due Diligence (IV)

- Identify & verify identity of natural persons (II)
  - documents required for verification:
    - ◆ for HK residents: a copy of ID card
    - ◆ for non-HK residents: a copy of valid travel document such as the “biodata” page of passport
    - ◆ residential address proof from a reliable source issued within the last 3 months (e.g. utility bill, bank statement)

(AML Guideline Chapter 4.8)

# Carrying out Customer Due Diligence (V)



- Identify & verify identity of corporations (I)
  - obtaining the information below:
    - ◆ full name
    - ◆ date and place of incorporation
    - ◆ registration / incorporation number
    - ◆ registered office address





# Carrying out Customer Due Diligence (VI)

- Identify & verify identity of corporations (II)
    - documents required for verification:
      - ◆ copy of CI & BR certificate
      - ◆ copy of M&A
      - ◆ ownership chart
- (AML Guideline Chapter 4.9)



# Carrying out Customer Due Diligence (VII)

- Identify & verify identity of beneficial owners
  - major shareholders:
    - ◆ for **normal risk** circumstances, all shareholders holding  $\geq 25\%$  of share capital / voting rights
    - ◆ for **high risk** circumstances, all shareholders holding  $\geq 10\%$  of share capital / voting rights
  - any individuals exercising ultimate control  
(AML Guideline Chapter 4.9.14)



# Special Requirements for Remittance Transactions

- outward remittance transaction  $\geq$  \$8,000
- identify & verify identity of the originator
  - name
  - ID
  - address
- date and time of receipt of instruction
- transaction amount
- recipient's name and address
- method of delivery

(AMLO Schedule 2 Section 13 / AML Guideline Chapter 11)



# Special Requirements for High Risk Circumstances

- obtaining information on the source of wealth and funds
- approval of senior management
- obtaining additional information with enhanced monitoring
- all high-risk customers should be subject to a minimum annual review (up-to-date information)  
(AML Guideline Chapter 4.11)



# Ongoing Monitoring of Business Relationship



# Ongoing Monitoring of Business Relationship

- reviewing from time to time documents, data and information relating to the customer
- exception reports will help MSOs stay apprised of operational activities.
- monitoring the activities of the customer to ensure their consistency with the nature of business, the risk profile and source of funds
- taking additional measures when monitoring business relationships that pose a higher risk.

(AML Guideline Chapter 5)



# Record Keeping



# Record Keeping

- Customer records
  - the original or a copy of the documents, and a record of the data and information, obtained in the course of identifying and verifying the identity of the customer and/or beneficial owner of the customer
  - should be kept throughout the business relationship with the customer and for a period of SIX years after the end of the business relationship

(AML Guideline Chapter 8.3 – 8.4)





# Record Keeping

- Transaction records
    - the original or a copy of the documents, and a record of the data and information, obtained in connection with the transaction
    - for a period of SIX years after the completion of a transaction, regardless of whether the business relationship ends during the period
- (AML Guideline Chapter 8.5 – 8.6)



# Staff Training



# Staff Training

- to ensure relevant staff receive adequate training in carrying out their particular roles with respect to AML/CFT
- the timing and content of training packages for different groups of staff will need to be adapted by individual company for their own needs
- the frequency of training should be sufficient to maintain the AML/CFT knowledge  
(AML Guideline Chapter 9)



# **Suspicious Transactions Reporting**



# Suspicious Transactions Reporting

- to ensure sufficient guidance is given to staff to enable them to form suspicion or to recognise when ML/TF is taking place
- should formulate a clear internal reporting procedures
- should appoint a MLRO as a central point for reporting suspicious transactions
- a disclosure should be made even where no transaction has been conducted in the event of suspicion of ML/TF  
(AML Guideline Chapter 7)





# Internal Monitoring System



# Internal Monitoring System

- conduct regular audits to test the procedures are adhered to throughout the business
- review and update of risk controls
- provision of regular and timely information to senior management
- training of employees on legal responsibilities and risk alert



# **Policy Statement**

## **Template**

### **For Reference Only**



**The End  
Thank You**

