Seminar for Money Service Operators (MSOs)

Money Service Supervision Bureau

May 2014

Anti-Money Laundering/ Counter-Terrorist Financing (AML/CFT) Systems

AML/CFT
Policies, Procedures and Controls

- to take all reasonable measures to ensure that proper safeguards exist to mitigate the risks of ML/TF
- to prevent a contravention of any requirement under Part 2 or 3 of Schedule 2
- to establish and implement adequate and appropriate AML/CFT systems taking into account factors including products and services offered, types of customers, geographical locations involved

(AML Guideline 2.1 - 2.2)

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:
  - customer
  - product/service
  - delivery/distribution channel
  - country/geographical location

Risk Identification & Assessment (II)

- Customer Risk (I)
  - customers with businesses that 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 (PEPs)

Risk Identification & Assessment (III)

- Customer Risk (II)
  - customers who are not local to the business
  - new customers/customers carrying out regular large transactions
  - non face-to-face customers
  - source of wealth cannot be easily verified

Risk Identification & Assessment (IV)

- Product/Service Risk
  - product/service that inherently have provided more anonymity
  - ability to pool underlying customers/funds

Risk Identification & Assessment (V)

- Delivery/Distribution 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 (VI)

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

  (AML Guideline 2.3 - 2.8 & 3.4 - 3.5)

Circular
30 January 2014

Money Laundering and Terrorist Financing Risks Associated with Virtual Commodities

- global attention to the ML/TF risks associated with virtual commodities
- to take all reasonable measures to ensure proper safeguards exist to mitigate the ML/TF risks that you may face in this regard taking into consideration the related developments
- high ML/TF risk situation : take additional measures to mitigate the ML/TF risk involved

Circular
21 March 2014

HKSAR on 14 March 2014

- warning the public of risks associated with any trading or dealing in virtual commodities
- MSOs
  - when establishing or maintaining business relationships with potential or existing customers who are operators of schemes or businesses related to virtual commodities
  - should exercise caution in assessing relevant ML/TF risks
  - take additional CDD measures
  - perform enhanced ongoing monitoring of activities for the account of any such customer to detect suspicious transactions

Statement
26 April 2014

In relation to "Bitcoin" and Money Service Operator Licence

The C&ED reminds licensed MSOs, applicants for an MSO licence and members of the public that, for the purposes of the AMLO, "Bitcoin" or other similar virtual commodities are not "money" and do not fall within the regulatory regime administered by the C&ED.

High-risk Situations

High-risk Situations

- obtaining additional information on the customer and updating more regularly the customer profile including the identification data
- obtaining additional information on the intended nature of the business relationship, the source of wealth and source of funds
- obtaining the approval of senior management to commence or continue the relationship
- conducting enhanced monitoring of the business relationship, by increasing the number and timing of the controls applied and selecting patterns of transactions that need further examination

(AML Guideline 4.11)

Ongoing Monitoring

Ongoing Monitoring (I)

- Continuously monitor business relationship with a customer by :
  - review from time to time CDD documents, data and information
  - scrutinize transactions with customers to ensure they are consistent with the customer's risk profile
  - identify transactions that are complex, large or unusual or patterns of transactions with no apparent economic or lawful purpose

(AML Guideline 5.1)

Ongoing Monitoring (II)

- Risk-based approach to monitoring
  - the extent of monitoring should be linked to the risk profile of the customer which has been determined through the risk assessment
  - must take additional measures when monitoring business relationships that pose a higher risk

    (AML Guideline 5.7 - 5.8)

Ongoing Monitoring (III)

- Methods and Procedures
  - should take into account the following factors
    - the size and complexity of its business;
    - its assessment of the ML/TF risks arising from its business
    - the nature of its systems and controls
    - the monitoring procedures that already exist to satisfy other business needs
    - the nature of the products and services
    - exception reports will help stay apprised of operational activities of the customer

      (AML Guideline 5.9)

Ongoing Monitoring (IV)

- examination of transactions that are complex, large or unusual, or patterns of transactions which have no apparent economic or lawful purpose
- findings/outcomes properly documented in writing
- proper records of decision made, by whom, and rationale

(AML Guideline 5.10)

Ongoing Review

Ongoing Review

- adjust risk assessment of a particular customer from time to time or based upon information received from a competent authority
- review the extent of the CDD and ongoing monitoring to be applied to the customer
- keep policies and procedures under regular review and assess risk mitigation procedures and controls are working effectively

Timing of Identification and Verification of Identity

Timing of Identification and Verification of Identity

- if cannot complete CDD, **must not** establish business relationship or carry out an occasional transaction
- assess whether this failure provides grounds for knowledge or suspicion of ML/TF and to report to JFIU

(AML Guideline 4.7)

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

Allocation of Responsibilities

Allocation of Responsibilities

- Senior Management
  - assess the risks the firm faces
- Compliance Officer
  - prevention and detection of ML/TF
- Money Laundering Reporting Officer
  - report suspicious transactions to the JFIU
- Frontline Staff
  - judge whether a transaction is suspicious

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)

A failure to disclose such suspicious transactions to the JFIU may amount to an offence under the Organized and Serious Crimes Ordinance, the Drug Trafficking (Recovery of Proceeds) Ordinance, or the United Nations (Anti-Terrorism Measures) Ordinance.

Thank You!